International Journal of Cooperative Information Systems

World Scientific
www.worldscientific.com

ASSESSMENT OF ENTERPRISE INFORMATION SECURITY -THE IMPORTANCE OF PRIORITIZATION -

PONTUS JOHNSON

Royal Institute of Technology
100 44 Stockholm, Sweden
pj101@ics.kth.se

ERIK JOHANSSON

Royal Institute of Technology
100 44 Stockholm, Sweden
erjo101@ics.kth.se

Received
Revised

Assessing the level of information security in an enterprise is a serious challenge for many organizations. One problem with such assessments is that there are various views on what, exactly, should be measured. There are different opinions on what the constituent parts of enterprise information security are and what these parts' relative importance is.
Addressing that problem, this article presents an operational definition and prioritization of the field of enterprise information security. First, the article proposes a framework for capturing the semantic essence of enterprise information security. Then, the relative weights of the framework's subdomains are quantified. Two methods for prioritization are used to obtain the weights. The results demonstrate to what extent different standards committees, guideline authors and expert groups differ in their opinions on what the important issues are in enterprise information security.
As prioritization sources, the ISO/IEC 17799, the NIST SP 800-26, the ISF standards committees, the CMU/SEI OCTAVE framework authors and an expert panel at the Swedish Information Processing Society (DFS) are considered.
To demonstrate the practical consequences, the effects of varying prioritizations on the enterprise information security assessment results in a European energy company are presented.

Keywords: Enterprise Information Security; Security Assessment; Prioritization.

1. Background to Research

This paper presents results from an on-going research project that focuses on the development of a method for the assessment of Enterprise Information Security. The project is part of a comprehensive research program, the Enterprise Architecture Research Program (EARP) at the Royal Institute of Technology (KTH) in Stockholm Sweden. EARP explores the discipline of Enterprise Architecture as an approach for managing the company's total information system portfolio. The company's primary stakeholder for the Enterprise Architecture is the Chief Information Officer (CIO) who is responsible for the management and evolution of the enterprise information system. The overall goal of the research program is to develop architecture-based tools and methods for planning and decision making on enterprise-wide information system.[1]

Information security has become an increasingly important system quality that has to be carefully managed on the enterprise level. Although Enterprise Information Security today is one of the most central areas for enterprise IT management, the topic still lacks good support for decision making on top-management level (i.e. the CIO level).[2] Good decisions require good information. Consequently a credible and usable method for assessing the current state of Enterprise Information Security is desirable.

1.1. *Purpose and Scope*

The purpose of the overall research project is to develop an quantitative, cheap, credible and prescriptive method for the assessment of Enterprise Information Security (herein denoted as the EIS assessment method).

To determine the assessment objectives unambiguously, this article defines the area of Enterprise Information Security in terms of a tree-structure. In order to determine the relative weights of the various parts of the tree, the structure is then prioritized, using two different methods and diverse sources (standards/guidelines and expert groups).

1.2. *Outline*

The next section gives a brief presentation of the EIS method as a whole. The rest of this paper takes a closer look at the definition and prioritization of the field of enterprise information security. Section 3 introduces the Architecture Theory Diagram (ATD), which is a structure for defining the area. In Section 4, the method employed for arriving at a definition is reviewed. The actual definition of enterprise information security is then presented in Section 5. Section 6 describes two methods for prioritization and Section 7 presents the prioritization results. As a demonstration, a real assessment of the level of enterprise security in a large European energy company is presented in Section 8. Finally, in Section 9, the paper is concluded.

2. Presentation of the Method

In this section, the fundamental ideas behind the EIS assessment method are introduced. The purpose of the EIS assessment method is to perform an assessment of the level of enterprise information security at a given company. There are some important requirements that separate this security assessment method from others. Firstly, the assessment result is to be presented as a *single value* on a scale, e.g. a percentage score. Secondly, an explicit requirement on the method is that the *credibility* of the assessment score is presented. Thirdly, the assessment procedure should be as *cost-effective* as possible. In particular, this relates to the cost of searching for information in the company under review. Finally, the method should be prescriptive, i.e., once the assessment is completed, the method should indicate clearly how the level of EIS could be improved.

Section 2.1 presents an idealized approach for determining the level of enterprise information security. In the subsequent subsections, this idealized approach is successively refined by considering the relative weights of different parts of the area, the credibility of the assessment results, and the effort of performing the assessment

2.1. *Devising a Score for EIS*

When attempting to assess enterprise information security, the first problem encountered is what to assess; i.e. what exactly is the area of inquiry? The natural answer is to rely on established knowledge in terms of literature on the subject. When searching the available literature on information security, however, this turns out to be a wide and oftentimes contradictory collection of books, reports and articles. However, the arguably most well-established sources on enterprise information security are international and national standards on the topic, cf. Refs. 3 - 6.

It would be desirable to use these as a base in an evaluation of the level of enterprise information security. If a company satisfied all standards, it would arguably have a very high degree of information security. Assuming that these standards are correct and complete, they could also be used to define the area of inquiry. In the present approach, the most highly cited standards within the area have been compiled into a database of EIS questions (and requirements, which have been rephrased into questions), see Figure 1.

An example of a question might be: *"To what extent are intrusion detection tools installed on the systems?"*. Currently, the database is comprised of 1114 such questions, and together they may be viewed as defining what Enterprise Information Security is.

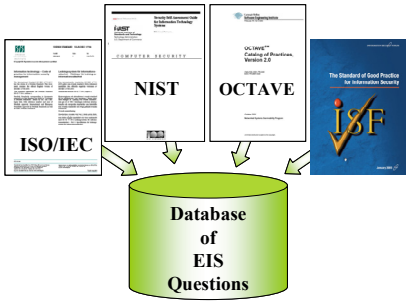

Figure 1. The area of information security is defined by several standards, which have been compiled into a database of EIS questions.

If we, for some specific enterprise, obtained positive answers to all the questions in the database, the company would arguable merit the highest EIS score. Inversely, if we obtained negative answers to all questions in the database, the company would arguably deserve the lowest EIS score. The database of questions might thus be employed to assess the level of information security on a simple ternary scale, where companies satisfying all questions/requirements obtained the score 2, companies satisfying some requirements obtained 1 and companies satisfying none obtained 0.

However, since most companies would end up in category 1 on the ternary scale, we would like to increase the resolution of the scale. But if we obtained a mix of positive and negative answers, we might not be able to determine an EIS score, because 1) the answers may not be on the same scales, and 2) different questions may be more or less important in relation to each other. In order to address the first concern, answers are mapped to a standard scale. To address the second issue, it is necessary to assign different priorities to all the questions respectively. In order to avoid prioritizing all questions in the database individually we may classify them and prioritize the classes. The problem then, is to find a sound classification of the large number of questions. This issue and the issue of assigning priorities to the classification constitute the main contributions of this article. They will therefore be further considered in subsequent sections. For this introductory review, suffice to mention that the classification is presented in a hierarchical structure called Architecture Theory Diagrams (ATDs), see Figure 7 in Section 7.1.

2.2. *An Credible but Expensive Answer*

The most simplistic approach to obtaining an EIS score would be to simply ask all questions and aggregate the answers according to the abovementioned prioritized hierarchical classification, as a kind of weighted mean. There is, however, a complication with this approach: there is a cost associated with obtaining a credible answer to an individual question. The more effort we spend on corroborating the answer by alternative sources etc., the more credible it becomes, see Refs. 7 and 8. The relation between credibility of the result and effort spent on obtaining it is thus increasing.

Furthermore, it is conceivably resource demanding to obtain even low-credibility answers for the more than thousand questions found in the EIS database. By settling for less than all answers, credibility of the EIS score is compromised. Thus, also the relation between credibility and number of questions is increasing, as indicated in Figure 2.

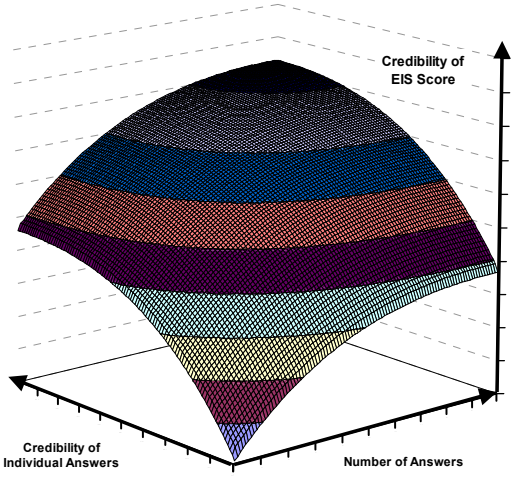

Figure 2. The total credibility of the EIS score is dependent on the total number of questions answered as well as the credibility of individual answers.

2.3. *Trading Credibility against Cost*

To make an assessment manageable, we can limit the cost of answering questions by 1) selecting a limited set of questions randomly and 2) using a fixed search cost for each answer. The overall credibility of the EIS score will then be dependent on the credibility of individual answers as well as total number of answered questions.

In this approach, we can thus improve the credibility of the EIS score by increasing the effort of answering questions. Effort could be spent on increasing either the quality or the quantity of the answers. In order to make use of these insights, we must be able to estimate the credibility of the EIS score and the individual answers. Credibility estimations are further elaborated in Ref. 9.

2.4. *Increasing Credibility at Constant Cost*

In contrast to the simple approach presented above, we here propose a more elaborate option where the credibility is improved *without* increasing the effort of answering questions. In order to accomplish this, three criteria are employed. They are briefly presented below.

2.4.1. *Choose Important Questions in Favor of Unimportant Ones*

By favoring highly prioritized questions, we can improve credibility at a given effort level, see Figure 3. Subsequent sections of this article consider the issue of prioritization.

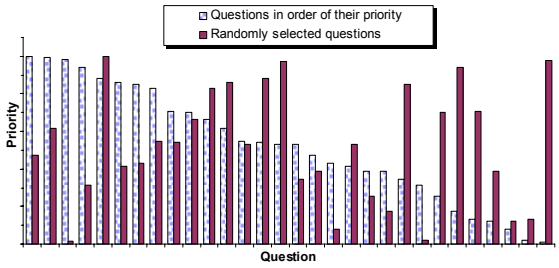

Figure 3. By answering questions in order of their priority instead of selecting them randomly, the credibility of the assessment can be improved at constant effort.

2.4.2. *Choose Cheap Questions in Favor of Costly Ones*

By favoring easy-to-find questions (those with a favorable credibility-versus-effort curve), we can improve the credibility of the EIS score at a given effort level, see Figure 4a. Methods for minimizing the effort by choosing the cheap questions are further elaborated in Ref. 11.

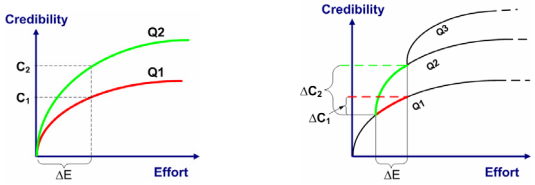

Figure 4. (a) When answering questions it is preferable to choose the one associated with the Q2 curve than the one associated with the Q1 curve. The question with a favorable credibility-versus-effort curve improves credibility of the EIS score most for a given effort ΔE. (b) Maximizing the credibility is a trade-off between the effort spent on a specific question vs. the effort spend on answering several questions. It is at some point better to spend the effort ΔE on answering a new question Q2 than on improving the credibility of the answer to an old question Q1.

2.4.3. *Trade-off Individual Credibility with Statistical Credibility*

By optimizing the effort spent on 1) improving credibility of individual questions and 2) answering more questions, we can improve the credibility of the EIS score at a given effort level. Figure 4b illustrates how a fixed effort ΔE increases the credibility. The increase is ΔC_1 if spent on a question Q1 (that has already been answered to a certain credibility level). The increase is ΔC_2 if spent on a new question Q2 that has not been considered yet.

The different aspects of the EIS assessment method presented in this brief review are offered in greater detail in Refs. 9 - 12. The present paper focuses on the aspects of definition and prioritization of the area of Enterprise Information Security.

3. The Architecture Theory Diagram

In order to assess, it is fundamental to be able to clearly define the assessment topic. In this section, we present the *architecture theory diagram* (ATD) as a tool for such definitions. For a more comprehensive presentation of ATDs, see Refs. 13 and 14. In the next section, we detail the process of ATD construction specifically for Enterprise Information Security.

3.1. *A Brief Description of the ATD*

You cannot control what you cannot measure and you cannot measure what you cannot define. The ATD presents how intangible system properties, such as enterprise information security, can be assessed by means of more concrete properties. The ATD on Enterprise Information Security is presented in Figure 7 in Section 7.1 (the details of the EIS ATD will be further elaborated on in subsequent section). ATDs are constructed by a hierarchical decomposition of the top-level property (in our case Enterprise Information Security) into sub-components according to certain rules. This decomposition can be performed repeatedly in order to generate a tree-structured hierarchy. One may interpret each property in the subdivided tree as the aggregate of its underlying properties. By making the theory explicit the ATD facilitates both critical examination and reuse of the theory.

3.1.1. *The Abstract Property*

Properties in ATDs may be of different kinds. The abstract property is the property under investigation, i.e. Enterprise Information Security in this case. The purpose of assessment is to obtain a value for this property. Since the abstract property generally is not an operationalized property (cf. below), the measurement process is typically dependent on underlying properties.

3.1.2. *Operationalized Properties*

The value of an operationalized property is assumed to be measurable to people performing assessments according to the theory diagram. In particular, this means that the property is sufficiently well-defined to make probable that two independent inquiries would obtain the same measurement of the property. In our case, the questions in the theory database are considered operationalized.

3.1.3. *Intermediate Properties*

Intermediate properties are neither the abstract property nor operationalized properties. As with the abstract property, their measurement depends on underlying properties. Unlike the abstract property, the purpose of the investigation is not to find values for these properties; they are but means to an end.

3.1.4. *Priority*

The strength of relations in an architectural theory diagram may vary. Some properties affect each other much while others are less important. This strength may be indicated by various types of scales. In our case relational strength is indicated by a percentage scale.

4. Method for ATD Generation

This chapter presents how the ATD on Enterprise Information Security was constructed. The quality of the ATD is dependent on the selection of sources and the analysis of those sources. The first subsection in this chapter presents the selected sources and the second subsection gives a brief presentation of the steps to generate the ATD from those sources.

4.1. *The Selected Sources*

The selection of sources for the generation of the ATD was approached by extensive literature search in order to obtain the most relevant theory over the area. There is definitely no lack of standards, practices, and guidelines available for information security and related disciplines—in fact, in a recent list[15] of relative documents for information security, no less than 81 different sets of "best practices" could be found.
For the present ATD, the relevance of literature was determined by its:

(i) fit with respect to the intended scope;
(ii) scientific weight, e.g. by citation databases; and
(iii) degree of operationalization, i.e. the practical applicability.

A decision on the amount of literature that would constitute the base of the theory diagram had to be made. In the simplest case, only one reference could have been employed. However, in this research we wanted to receive a broader base for the area of enterprise information security, therefore four references from different organizations have been employed. They are briefly described below.

4.1.1. *ISO/IEC*

One of the most prominent sources, with respect to the subject of information security, is the International Standard 17799 *Information Technology - Code of Practice for Information Security Management*. This standard is jointly published by the *International Organization for Standardization (ISO*[*]*)* and the *International Electrotechnical*

[*] ISO, officially began its operations 1947, and is today the world's largest developer of standards. ISO is a non-governmental organization, a federation of the national standards bodies of more than 150 countries.

Commission (IEC[†]). This standard, like its predecessor the *British Standard 7799*, sets the requirements for an information security management system or process. It is intended to be used by organizations for the identification and management of the range of threats to which information is routinely subjected. This standard is organized into 10 coverage areas: security policy, organization of assets and resources, asset classification and control, personnel security, physical and environmental security, communications and operations management, access control, systems development and maintenance, business continuity management, and compliance, see refs. 3. The International Standard 17799 is widely used and thus a natural choice for the theoretical base of this work.

4.1.2. *NIST*

Another source of relevant practices is the *National Institute of Standards and Technology (NIST)* 800-level series on information security. NIST, founded in 1901, is a non-regulatory federal agency within the U.S. Commerce Department's Technology Administration.

One of NIST's published special publications (SP) on the topic of information security is the SP 800-26 *Security Self-Assessment Guide for Information Technology Systems*[4], released in 2001. This self-assessment guide utilizes an extensive questionnaire containing specific control objectives and techniques against which an unclassified system or group of interconnected systems can be tested and measured.

4.1.3. *ISF*

The *Information Security Forum (ISF)* is an international association of over 270 leading companies and public sector organizations that fund and cooperate in the development of practical research in information security and best practices in IT security and information risk management. The ISF produces the *Standard of Good Practice for Information Security*[5] (The Standard). The Standard is based on 16 years of ongoing research and is positioned as an aid to organizations in understanding and applying best practices for information security. Since it addresses security from a business perspective, The Standard appropriately recognizes the intersection between organizational drivers and security drivers, and thus is a good fit for the present focus on enterprise information security.

4.1.4. *OCTAVE*

The *Software Engineering Institute (SEI)*, a federally funded research and development center in U.S. operated by *Carnegie Mellon University (CMU)* have released the *Operationally Critical Threat, Asset, and Vulnerability Evaluation*[SM] *(OCTAVE®)* approach. The OCTAVE approach focuses on organizational risk and strategic, practice-

[†] International standardization began in the electrotechnical field: the IEC was established in 1906, and is a global organization that prepares and publishes international standards for all electrical, electronic and related technologies.

related issues, balancing operational risk, security practices, and technology. It is driven by two of the aspects: operational risk and security practices. Technology is examined only in relation to security practices, enabling an organization to refine the view of its current security practices. The OCTAVE approach is self-directed - a small team of people from the operational (or business) units and the IT department work together to address the security needs of the organization. The team draws on the knowledge of many employees to define the current state of security, identify risks to critical assets, and set a security strategy. By using this approach, an organization makes information-protection decisions based on risks to the confidentiality, integrity, and availability of critical information-related assets.

In year 2001 CMU/SEI released the second version of the *OCTAVE Catalog of Practices,* which have been used in this work. [6]

4.2. *Source Analysis*

In order to transform the above standards into a synthesized ATD, a comprehensive syntactic and semantic analysis consisting of five steps was performed.

(i) Creation of a database
(ii) Listing of all words in the database
(iii) Clustering the synonyms as semantic units
(iv) Extracting the frequencies of semantic units
(v) Identification of dimensions

These five steps are briefly described in the next subsections.

4.2.1. *Creation of a Database*

All selected sources consist of different kinds of requirements and/or questions. These requirements/questions were compiled into a theory database in order to enable the upcoming analysis.

4.2.2. *Listing of all Words in the Database*

In order to capture the overall definition of the area, as characterized by the collection of theories, all words from the requirements/questions in the theory database were listed, since we assume that the most common words would reflect the most important part of the consolidated theory.

4.2.3. *Clustering of Synonyms as Semantic Units*

In the created list of words there were of course many words that need to be excluded, such as conjunctions and prepositions. Furthermore, semantically similar words were clustered. For instance, “staff” and “personnel” normally signify the same thing, consequently these should be bundled. Thereby a list of semantic units was created based on words with similar meaning.

4.2.4. *Extracting Frequencies of Semantic Units*

The number of instances of each individual semantic unit was extracted from the theory database. A list of these frequencies was created.

4.2.5. *Identification of Dimensions*

It was now possible to analyze the theory coverage of the different set of semantic units, by examining their frequencies of occurrence. The occurrences of a semantic unit in the database correspond to the size in its theory coverage.

These steps lead to the identification of large and individually independent dimensions of the topic, further presented in Section 5. All the requirements/questions of the unconsolidated theory diagrams become the bottom-level properties (questions) of the consolidated ATD.

5. Definition of Enterprise Information Security

The preceding chapters showed how the ATD was constructed from well-known sources. In this chapter the resulting ATD is presented.

5.1. *Dimensions of Enterprise Information Security*

The identification of dimensions described in subsection 4.2 resulted in three independent dimensions relevant for the assessment of Enterprise Information Security: *scope*, *purpose*, and *time*.

5.1.1. *Scope*

The first dimension is related to the *scope* of the security measurements, answering *how* the protection is implemented. The dimensional units are:

- *Technical*, i.e. information systems, information system infrastructure, hardware and software;
- *Organizational*, i.e. the policies, responsibilities, management and organizational processes to establish and maintain security and security awareness of employees;
- *Environmental*, i.e. the external factors and security, including systems protecting information systems and systems maintaining the environmental security such as fences and buildings.

5.1.2. *Purpose*

The second dimension is related to the *purpose* of the security measurements, answering *why* the protection is carried out. The dimensional units are:

- *Preventive*, i.e. requirements or actions intended or used to prevent or hinder; acting as an obstacle *(preventive measures)*;
- *Detective*, i.e. requirements or actions intended to discover or ascertain the existence of adverse events e.g. intrusion identification;

- *Responsive*, i.e. requirements or actions intended to respond to external adverse events (such as modification of information) and to maintain business continuity.

5.1.3. *Time*

The third dimension is related to the *time* aspects of the security activities, answering *when* the security-related actions are carried out. The dimensional units are:

- *Planning*, i.e. the initial activities and phases, e.g. planning, design, establishment, configuration, installation, initial risk analysis;
- *Operational*, i.e. the continuous activities and phases, e.g. operation and usage, monitoring, maintenance, observance, continuous risk analysis;
- *Controlling*, i.e. the follow-up activities and phases, e.g. verification and validations, audits and reviews (verifying the fulfillment and compliance), validation of risk analysis.

These three independent dimensions may be illustrated as a cube, see Figure 5.

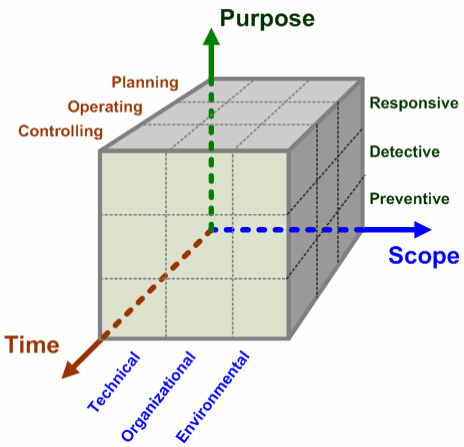

Figure 5. The Enterprise Information Security Cube is a framework for capturing the semantic essence of the EIS concept.

5.2. *The Architecture Theory Diagram for Enterprise Information Security*

The 27 identified subdomains of the Enterprise Information Security Cube may be translated into a four-level ATD. The dimensions represent the three main sublevels of Enterprise Information Security, see Figure 7 in Section 7.1. In the ATD, the *scope* dimension (i.e. technical, organizational, and environmental) is on the second level. On the third level the *purpose* dimension (i.e. preventive, detective, and responsive) is introduced and finally the *time* dimension (i.e. planning, operation, and controlling) is included on the fourth level. At the bottom of the hierarchy are the questions from the theory database, each question linked to a category of the ATD.

6. Method of Prioritization

As presented earlier, the EIS assessment method determines the level of EIS by posing a set of specific questions about the considered organization. In a simple assessment approach, the mean value of the answers can constitute the EIS score. However, certain questions are deemed more important than others. This implies that two different prioritizations of the same set of questions may result in completely different results. Taking this complication into account, we need to find a method to prioritize the questions. This section presents how this can be done. The next section details the results of such methods, i.e. actual prioritizations of the properties in the ATD.

6.1. *Problems to Address*

A problem with priorities is that they vary with the stakeholders and the context. There are three reasons for this variation. Firstly, priorities may vary because different stakeholders define the same area differently. For instance, some may feel that physical security is a part of enterprise information security while others do not. Secondly, given a definition, priorities may vary because different stakeholders have differing opinions on what really affects the enterprise information security. For instance, some may think that the most important determinant of enterprise information security is the quality of security-related technology within the enterprise, e.g. firewalls and intrusion prevention systems, while others believe that employee awareness is the main culprit. Thirdly, priorities can differ because what really affects enterprise information security may vary depending on the company and its context. For instance, certain organizations are prestigious targets for hackers, while others are not.

The first problem is addressed in Sections 4 and 5, where the EIS area is solidly defined. The second problem is addressed below by enabling a comparison between alternative views (theories) of what in fact does lead to high EIS. The third problem, the problem of context-dependent priorities, is addressed by offering two different methods for prioritization, as detailed further in the next section.

6.2. *Two Methods*

Two different methods for prioritizing the ATD on enterprise information security are presented here. The first method bases the priorities on general literature in the field; more specifically on the previously reviewed international standards for enterprise information security. This approach is suitable for general prioritizations irrespective of the particular context or enterprise. The second method is based on survey results, where the preferences of specific individuals or groups are used as a base for the prioritization. This approach is suitable for enterprise-specific or context-specific prioritizations.

6.3. *Theory-based Prioritization*

In Section 4, four highly cited, internationally recognized information security standards were used for defining EIS, see Refs. 3 - 6. These are now employed as sources for prioritizing the categories of the ATD.

If the source considers a certain category in many of its requirements, the category is arguably important. Therefore, the prioritization of a particular source may be obtained by counting the number of requirements or questions that treat different categories.

6.3.1. *Weight of Sources*

How do we know which sources, such as security standards, are important? A general academic approach to comparing literature is to consider the number of times the sources are referred to by other literature, i.e. the number of citations. Such numbers are readily available on the Internet[‡]. The resulting numbers of citations can then be translated into a weight of importance for the corresponding sources. An alternative option is to investigate the actual use of the sources at a number of organizations resulting in a practical weight of the theories. Yet another option is to assume that all the standards are equally important. In this work, the first alternative was chosen.

6.3.2. *Priorities of Questions in Sources*

Having weighed the sources, it is also necessary to consider the individual questions. The different sources do not have the same distribution of questions over the ATD categories. We therefore need to evaluate this distribution.

Equation 1 illustrates how to calculate the priorities for each one of the 27 EIS categories, $\omega(c)$, where c represents a specific category. This priority consists of two factors. The first factor is the weight of standard i in relation to the other standards, $\omega(i)$. The second factor is the weight of category c within standard i, $\omega_i(c)$. $\omega(i)$ is dependent on the number of citations for the *i:th* standard, C_i^{ref}, and the overall number of citations of all selected standards, C_{TOT}^{ref}. n is the total number of standards. $\omega_i(c)$ is dependent on the number of questions in category c in standard i, Q_i^c, and the total number of questions in the standard, Q_i^{TOT}.

$$\omega_c = \sum_{i=1}^{n} \frac{C_i^{ref}}{C_{TOT}^{ref}} \frac{Q_i^c}{Q_i^{TOT}}. \quad (1)$$

The aggregated value of the EIS scores, S^{EIS}, then becomes a weighted sum of each category's mean values, $\bar{V}_c$.

$$S^{EIS} = \sum_{c=1}^{27} \omega_c \bar{V}_c. \quad (2)$$

[‡] such as the "Computer and Information Science Papers CiteSeer Publications Research Index" at <http://citeseer.ist.psu.edu/cs> or the "Google Scholar" at <http://scholar.google.com/>

The theory-based approach is simple, straightforward and suitable for general prioritizations irrespective of the particular context or enterprise.

6.4. *AHP-based Prioritization*

In the second method, the preferences of specific individuals or groups of experts are used as a base for the prioritization. The employed method is based on the analytic hierarchy process, AHP[16]. In AHP, experts are subjected to pair-wise comparisons between categories to elicit their relative importance (cf. Table 1).

Table 1. Scale used in the AHP approach for pair-wise comparison of EIS categories.

Intensity of importance	Description
1	Of equal importance
3	Moderate difference in importance
5	Essential difference in importance
7	Major difference in importance
9	Extreme difference in importance
Reciprocals	If requirement *i* has one of the above numbers assigned to it when compared with requirement *j*, ther *j* has the reciprocal value when compared with *i*

Previous studies indicate that relative judgments tend to be faster and yield more reliable results than absolute judgments.[17] The AHP method thus reduces the prioritization effort.[18] However, since all unique pairs of EIS categories are to be compared, the required effort can still be substantial.

An important aspect for this practical approach of prioritization is the selection of respondents. Their experience is fundamental to minimize the judgmental errors. In the present context, suitable participants for the AHP-based prioritization could be security experts. However, when enterprise-specific prioritizations are needed, the opinions of respondents from the organization under examination are preferred.

7. Results of Prioritizations

This section presents the results of the prioritization of the EIS categories of the ATD. The first section presents the theory-based prioritization and the subsequent section presents an AHP-based prioritization developed in cooperation with the Swedish Information Processing Society (DFS).[19]

7.1. *Theory-based Prioritization using Security Standards*

A statistically significant value of the theory-based prioritization was established by selecting a random population of questions from each of the four security standards presented in Subsection 4.1 and categorizing them according to the 27 EIS categories. In Figure 6, the results are grouped by security cube dimension.

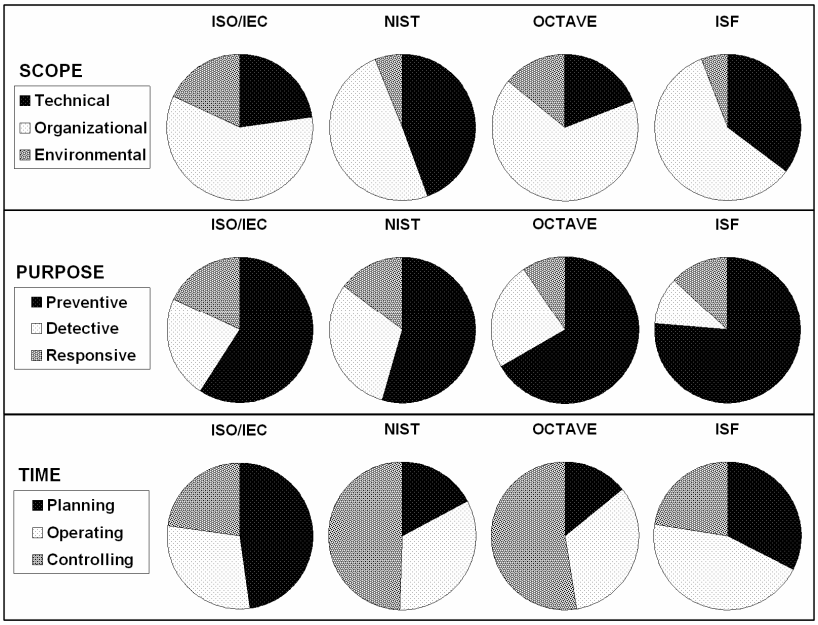

Figure 6. A comparison of the four security standards in relation to the identified dimensions of EIS.

This prioritization reveals variations of focus that are not immediately apparent when considering the different standards. In Figure 6 we thus find evidence for the proposition that there is no consensus among standards on the definition of EIS. We note that the standards are in acceptable agreement with respect to the *Purpose*-oriented dimension but not so with respect to the *Time*-oriented dimension, e.g. ISO/IEC stresses *Planning* more than *Controlling* while NIST displays the opposite emphasis. Another interesting observation is the general focus on organizational aspects of the Enterprise Information Security, e.g. governance and knowledge issues.

Aggregating the priorities of the security standards according to Subsection 6.3 and presenting the results in the form of an ATD, we obtain Figure 7.

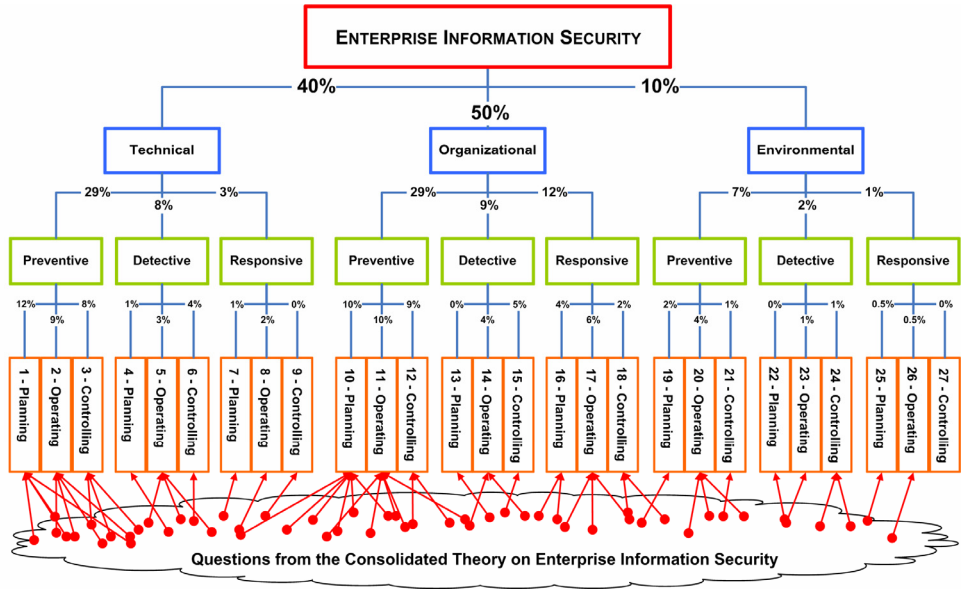

Figure 7. Illustration of the aggregated theory-based prioritized ATD on Enterprise Information Security (EIS). The numbers indicating the overall share of the theory database on EIS.

The ATD shows that *Organizational-Preventive-Operating* (i.e. EIS category 11) is more important than *Technical-Responsive-Controlling* (i.e. EIS category 9). This means that questions like – "Do security strategies and policies take into consideration the organization's business strategies and goals?" are considered more important than questions like – "Are back-ups verified to ensure that back-up versions can be restored successfully?"

7.2. *AHP-based Prioritization at the Swedish Information Processing Society*

Another kind of prioritization is obtained by letting practical experience from experts drive the ranking of the EIS categories. For the prioritization reported here, the respondents were chosen from a network of information security experts at the Swedish Information Processing Society (DFS).[19] 24 experienced information security consultants/auditors participated in a workshop where an AHP-based prioritization was carried out using a computer-based tool from Focal Point.[20] The expert's prioritization of the EIS categories is presented in Figure 9.

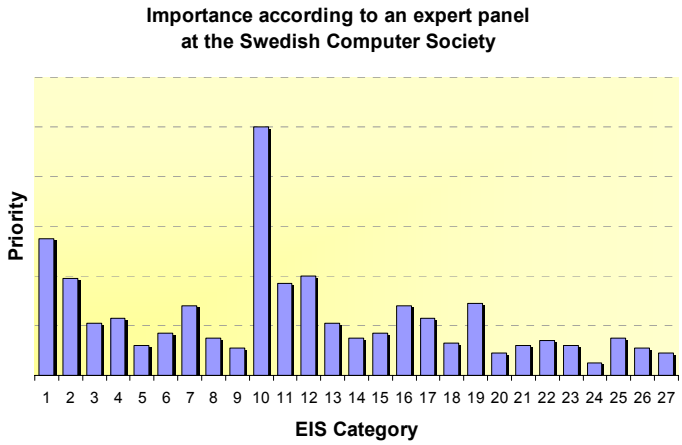

Figure 8. Illustration of the prioritization of the ATD on Enterprise Information Security (EIS) according to an expert panel at the Swedish Computer Society. The numbers denote the category in the ATD on EIS.

According to the expert panel workshop at the Swedish Information Processing Society the most important EIS categories are *Organizational–Preventive–Planning, Technical–Preventive–Planning,* and *Organizational–Preventive–Controlling.* The experts thus promote the preventive measures and the planning phase.

7.3. *Comparison of the Prioritizations*

Figure 9 compares the priorities of the security standards with the priorities of the security experts. If the two prioritizations had been identical, all the categories would have corresponded to a diagonal line.

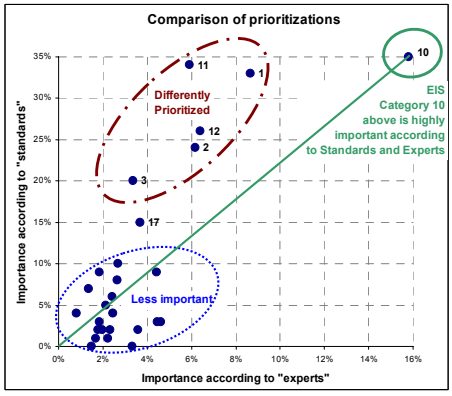

Figure 9. Importance of EIS categories according to experts within the Swedish Information Processing Society. Along the x-axis vs. the importance according to security standards along the y-axis.

We note that the experts 'agree' with the security standards with regard to the most important category, i.e. *Organizational-Preventive-Planning* (EIS category 10, cf. Figure 7). The largest deviation between the two prioritizations is the EIS category 11, i.e.

"Organizational-Preventive-Operating". The experts rank its relative importance as 40 % of the most important while the standards rank it almost as high as the most important EIS category.

8. Assessing Enterprise Information Security

In the preceding chapters we have demonstrated how it is possible to generate a prioritization of Enterprise Information Security by using theory from well-known sources and by expert elicitation. Now we have a clear, quantitative, prioritized and comprehensive definition that enables us to assess the enterprise information security of a given company. This section presents a survey which demonstrates the applicability of the prioritized ATD as a tool for Enterprise Information Security level assessment.

8.1. *Background to Case*

8.1.1. *The Enterprise*

The assessment was carried out at one of the largest electric utilities in Europe. The Chief Information Security Officer (CISO) wanted to assess the difference in the level of Enterprise Information Security between two subsidiaries of the enterprise. The two subsidiaries are, in this paper, denoted Company A and Company B.

8.1.2. *Data Collection*

The idea of the assessment was to generate an indicative answer within a short time frame. To that purpose, a set of questions was selected randomly from the theory database. These were then used in a self-assessment questionnaire. The questionnaire consisted of 28 questions, representing the major part of the ATD on EIS, see Ref. 9.

A top-level manager from each of the companies responded the questionnaire. The respondents were carefully chosen; both had comparable background and position at the two companies and they were familiar with the area of concern for the questionnaire.

The answers from the questionnaire were aggregated according to the prioritized ATD for each company respectively. The EIS score was then compared between the two companies, thus indicating the differences between the two companies.

8.2. *Results from the Assessment*

The assessment results from this survey consist of EIS scores indicating that there is a difference in the level of enterprise information security between the two subsidiaries, companies A and B. Figure 10 presents how the EIS scores vary depending on what source of prioritization is chosen. The expert prioritization generates moderate scores, while the ISF and the NIST standards' prioritizations generate comparatively high scores. We find that irrespectively of which prioritization source is chosen, company B obtains a higher EIS score than company A.

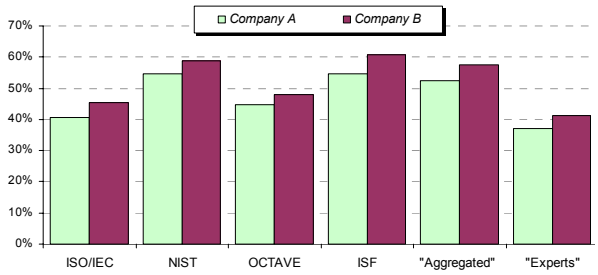

Figure 10. Comparison of the EIS score depending on the selected source for evaluation. The "Aggregated" is the overall aggregated theoretical-based priority as presented in Figure 7 and the "Experts" is the importance according to experts within the Swedish Information Processing Society.

8.3. *Comparison between Categories of the ATD*

A closer comparison of the results reveals further differences between the different sources used for prioritization. In Figure 11, the EIS assessment results for one single category of the ATD are presented; the EIS category 12, i.e. *"Organizational-Preventive-Controlling"*. Note the difference in assessment result when prioritizing according to NIST as compared to the other sources of prioritization.

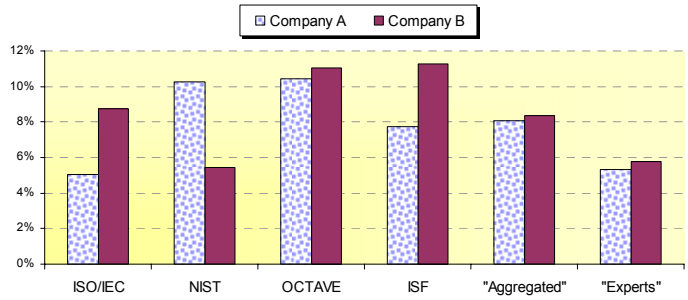

Figure 11. Illustration of the differences in the detailed assessment results between Company A and B. This observation is made by considering only EIS category 12, i.e. *"Organizational-Preventive-Controlling"*. Note the difference in assessment results when prioritizing according to NIST as compared to the other sources of prioritization.

8.4. *Discussion*

The results indicate that the perceived level of enterprise information security depends on the source used for the assessment. For instance, the difference in an EIS assessment between company A and company B could be less than 5% or more then 20%, depending on the chosen source of prioritization. These variations indicate a need for a common base for the EIS assessment. In this case, we suggest using the proposed aggregated prioritization where all the sources have been consolidated.

9. Summary

This article has presented results from on-going research on a method for assessment of Enterprise Information Security (EIS). The article proposed a framework for capturing the essence of enterprise information security. Two approaches for managing the problem of prioritizing a broad area such as EIS were then proposed. First, the concept of theory-based prioritization was introduced as a tool for objectively selecting the most important requirements for the EIS assessment. This approach is suitable for general prioritizations irrespective of the particular context or enterprise. The second method is based on the Analytic Hierarchy Process, AHP, where the preferences of specific individuals or groups are used as a base for the prioritization. This approach is suitable for enterprise-specific prioritizations. The actual results of these two prioritization methods were presented in the article and the feasibility of the general approach was demonstrated in a case study assessment of the Enterprise Information Security in one of the largest electric utilities in Europe.

Acknowledgements

The authors would like to thank Mårten Simonsson and Mathias Ekstedt for helpful comments and suggestions.

References

1. P. Johnson and M. Ekstedt, *The Grand Unified Theory of Software Engineering*, (Preprint, ISBN 91-974620-1-2, Royal Institute of Technology, Stockholm, 2005).
2. P. Johnson, et al., Using Enterprise Architecture for CIO Decision-Making: On the importance of theory, in *Proc. of the 2nd Annual Conference on Systems Engineering Researc*h, (2004).
3. ISO/IEC International Standard 17799:2000 *Information Technology - Security techniques - Code of Practice for Information Security Management* (2000).
4. NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems, National Institute of Standards and Technology, (2001).
5. Information Security Forum (ISF), *The Standard of Good Practice for Information Security* (2003), http://www.isfsecuritystandard.com.
6. C. Alberts, A. Dorofee, and J. Allen (2001a), *OCTAVE Catalog of Practices*, Version 2.0, Technical Report CMU/SEI-2001-TR-020 Carnegie Mellon University Software Engineering Institute, (2001).
7. S. L. Pfleeger, in *Soup or Art? The Role of Evidential Force in Empirical Software Engineering*, IEEE Software Volume 22, Issue 1, (2005) pp. 66–73.
8. R. K. Yin, *Case Study Research: Design and Methods*, (2nd ed., Sage Publications, 1996).
9. E. Johansson and P. Johnson, Assessment of Enterprise Information Security - An Architecture Theory Diagram Definition, in the *Proc of the 3rd Annual Conference on Systems Engineering Research*, (New York, March, 2005).
10. E. Johansson and P. Johnson, Assessment of Enterprise Information Security - Estimating the Credibility of the Results, in *Proc. of the Symposium on Requirements Engineering for Information Security*, (Paris, August, 2005).

11. E. Johansson, M. Ekstedt and P. Johnson, Assessment of Enterprise Information Security - The Importance of Information Search Cost, in *Proc. the 39th Hawaii International Conference on System Sciences*, (Hawaii, January, 2006).
12. E. Johansson, *Assessment of Enterprise Information Security – How to make it Credible and Efficient,* Ph.D. Thesis, Royal Institute of Technology (2005).
13. P. Johnson, M. Ekstedt, E. Silva, and L. Plazaola, Using Enterprise Architecture for CIO Decision-Making: On the importance of theory, in *Proc. of the 2nd Annual Conference on Systems Engineering Research*, (2004).
14. M. Ekstedt, P. Johnson, Å. Lindström, M. Gammelgård, E. Johansson, L. Plazaola, and E. Silva, Consistent Enterprise Software System Architecture for the CIO – A utility-Cost Approach, in *Proc. of the 37th annual Hawaii International Conference on System Sciences*, (Hawaii, USA, 2004).
15. Corporate Information Security Working Group, *Information Security Management References*, Adam H. Putnam, Chairman; Subcommittee on Technology, Information Policy, Intergovernmental Relations & the Census Government Reform Committee, U.S. House of Representatives, (2004).
16. T. L. Saaty, *The Analytic Hierarchy Process*, (McGraw-Hill, New York, 1980).
17. J. Karlsson, Software Requirements Prioritizing, in *Proc. of the 2nd IEEE International Conference on Requirements Engineering* (1996) pp. 110–116.
18. J. Karlsson, et al., An evaluation of methods for prioritizing software requirements, *in Information and Software Technology 39* (1998) pp. 939–947
19. Swedish Information Processing Society (2005), http://www.dfs.se.
20. Focal Point AB, Linköping, Sweden (2005), http://www.focalpoint.se.