Interactive Selection of ISO 27001 Controls under Multiple Objectives

Thomas Neubauer, Andreas Ekelhart, and Stefan Fenz

Abstract IT security incidents pose a major threat to the efficient execution of corporate strategies. Although, information security standards provide a holistic approach to mitigate these threats and legal acts demand their implementation, companies often refrain from the implementation of information security standards, especially due to high costs and the lack of evidence for a positive cost/benefit ratio. This paper presents a new approach that supports decision makers in interactively defining the optimal set of security controls according to ISO 27001. Therefore, it uses input data from a security ontology that allows the standardized integration of rules which are necessary to model potential countermeasure combinations based on the ISO 27001 standard controls. The approach was implemented into a tool and tested by means of a case study. It not only supports decision makers in defining the controls needed for certification but also provides them with information regarding the efficiency of the chosen controls with regard to multiple definable objectives.

1 Introduction

IT security incidents such as computer virus contaminations and unauthorized access to information, caused total losses of about 52 million US dollars among 313 U.S. respondents in 2005, coming from the commercial and governmental sector [12]. The Information Security Breaches Survey 2006 [21] estimates the overall costs of U.K. security breaches, mainly caused by virus infection and disruptive

Thomas Neubauer
Secure Business Austria, Vienna, Austria, e-mail: tneubauer@securityresearch.ac.at

Andreas Ekelhart
Secure Business Austria, Vienna, Austria, e-mail: aekelhart@securityresearch.ac.at

Stefan Fenz
Secure Business Austria, Vienna, Austria, e-mail: sfenz@securityresearch.ac.at

software, in the order of ten billion pounds per year. To protect their organization against such threats, 41 percent of U.K. businesses utilize an IT service provider or consultancy, 46 percent an internal audit function, and 42 percent personal contacts within the business or security community [21]. Only 7 percent of U.K. businesses carried out certification initiatives [21], in terms of BS7799 [4], ISO 17799 [14] or ISO 27001 [15] to strengthen the security of their processes and systems. Nine-tenths of businesses that have implemented an information security standard benefit in the following ways: (1) raising staff awareness, (2) pushing security up to the management agenda, (3) better business continuity, (4) formal accreditation, and (5) marketing reasons [21].

Most organizations carry out certification initiatives to become more commercially acceptable in sensitive business sectors (e.g., financial or health sector) or to comply to legal regulations such as Basel II [3] or the Sarbanes Oxley Act [22]. Especially in highly integrated businesses it is crucial that business partners can trust each other regarding the correct implementation of IT security measures in order to ensure that the integration of external IT services does not pose a risk to the own organization. However, in spite of these benefits, most companies refrain from the implementation of information security standards, especially due to high costs, the bureaucratic certification process and the lack of methods for measuring the cost/benefit ratio [21]. The major problem with information security standards is their abstract control definition, which leaves space for interpretation. Not the standard, but the certification auditor decides if certain security measures are compliant to the standard or not. Organizations which are required to obtain a formal certification often focus on satisfying the auditor and forget to evaluate and subsequently implement the optimal security measures in line with their specific corporate requirements. But investments into security should precisely target a company's specific business needs (and not only the requirements of the certification), as competitive advantages can only be accrued by aligning security investments to the corporate business processes as well as strategic and legal objectives. Thus, companies often fail in introducing standards because their primary focus lies on fulfilling the requirements given by the auditors, while they are frequently unaware of the level of their capital expenditure and/or – even more importantly – whether these investments are effective (cf. [16]).

In order to address these reservations and demands outlined above, we developed a new (two-phase) approach that supports decision makers in interactively defining the optimal set of security safeguards according to ISO 27001. In the first step, the security ontology (cf. [8], [9]), which comprises knowledge about the IT security domain including relationships among threats, vulnerabilities, countermeasures, and assets, serves as a knowledge base for potential countermeasure implementations. By now we have incorporated relevant parts of the German IT Grundschutz Manual [5] into the security ontology, to provide the organization with fundamental information security knowledge. While the initial ontology creation step has to be conducted by information security experts, the final information security knowledge base can be reused without expert support. Using an ontological knowledge base allows to model the IT security domain in a standardized way, enables ontological

reasoning support to maintain consistency, and enables the standardized integration of rules which are necessary to model potential countermeasure combinations. In the second step, Atana (a decision support approach which is derived from "AlTernative ANAlysis"; cf. [17], [18], [19]) determines solution alternatives that are both feasible with respect to given constraints and Pareto-efficient with respect to a number of objectives that have been identified as the most relevant ones for the given decision setting. Furthermore, Atana supports decision makers such as the Chief Security Officer in interactively exploring the determined solution space until they find their individually "best" solution. This paper describes the new approach and provides a case study.

2 Ontology-based Determination of Security Controls

Checklist-based tools are one approach to support the certification process. The assigned employee completes a questionnaire which reveals potential weaknesses and provides corresponding security recommendations. The questions, as well as the pre-defined sets of recommendations, are often based on best-practices. One weakness of checklists is that they usually offer general, high-level recommendations and cannot support organization specific threat scenarios. Furthermore, no underlying data model exists, which defines connections between the involved entities explicit to allow modification and reuse. Information security standard support tools (e.g., GSTool or EBIOS) are a further certification assistance possibility. Such tools facilitate a structured approach to comply to a defined certification standard, but cannot assist in the actual decision for appropriate security measures, as only the high-level control definitions are presented. To support the certification process in a standardized way, a conceptual and machine-readable model of IT security is required. Such a model has to incorporate best-practice knowledge about threats, threatened infrastructure classes, vulnerabilities, and countermeasures. One possibility to model the IT security domain and make it accessible for machines are ontologies. According to Gruber [13] an ontology is the explicit formal specification of the terms in the domain and the relations among them.

2.1 Security Ontology

We utilized the security ontology classification proposed in [8], [9], [10] which is based on the security relationship model presented in the National Institute of Standards and Technology Special Publication 800-12 [20]. Figure 1 shows the high-level concept of the ontology in which threats, vulnerabilities, controls and their implementation (safeguards) are the pivotal elements: a threat represents, through an existing vulnerability, any potential danger to the organizations' assets and affects specific security attributes (confidentiality, integrity, and/or availability). To pose a

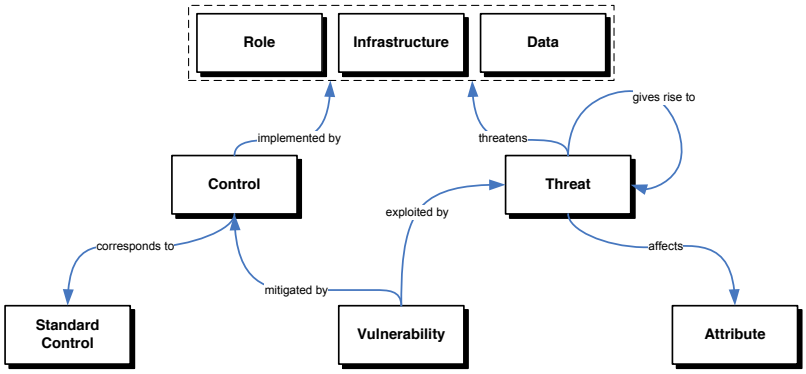

Fig. 1: Conceptual model of IT security

risk to an organization, a threat has to exploit a vulnerability, via a physical, technical or administrative weakness, and cause damage to defined assets. Controls have to be put into place to mitigate an identified vulnerability and to protect the corresponding assets by either preventive, corrective or detective measures. Each control is implemented by role, infrastructure, or data concepts or combinations thereof. Controls are derived from best-practice and information security standard controls (e.g., German Baseline Protection Manual, ISO 27001, or EBIOS) to ensure that the knowledge is widely accepted. The controls are modeled on a highly granular level and thereby reusable for different standards. The ontology follows the OWL-DL standard [24] and ensures that the knowledge is represented in a standardized and machine-readable form. As already mentioned, controls are implemented by role, infrastructure, or data concepts or combinations thereof. The connection between the control and its implementation (role, infrastructure, and/or data) is realized by a 1:n relation. Controls can be implemented in different ways. Therefore, we utilized the concept of OWL property restrictions in order to express these relationships in an ontological form. The universal OWL property restriction ($\forall$) is used to constrain the 'implementation' side to specific concepts. For example, to implement the *Access Regulation Control* a security guard, an entry checkpoint, or an access system is required, which is expressed as follows:

$$\forall\ \textit{sec:implementedBy only}\ (\textit{ent:SecurityGuard} \vee \textit{ent:AccessSystem} \vee \textit{ent:EntryCheckpoint})$$

Up to that point, the ontology is aware of which concepts (Role, Infrastructure and/or Data) are required to implement a certain control, but a description of the possible combinations is still missing. Therefore, we utilized the existential OWL property restriction ($\exists$), which states that at least one value for that property is of a certain type [24].

For example, the *Access Regulation Control* requires in all implementation variations an access system and either a security guard or an entry checkpoint:

$\exists$ *sec:implementedBy some ent:AccessSystem*
$\exists$ *sec:implementedBy some (ent:SecurityGuard* $\vee$ *ent:EntryCheckpoint)*

On this account, two possible implementation combinations are possible, namely access system and security guard, or access system and entry checkpoint.

The security ontology provides a set of evaluation criteria (benefit and resource categories) and a list of potential investment candidates including potential countermeasure implementations that are needed for the definition and selection of Pareto-efficient solutions (described in the following subsections). Each of these potential investment candidates is rated in every of the defined benefit and resource categories. The data needed for the rating is taken from the security ontology which contains specifications from the providers of the potential investment candidates, empirical evaluations and experience from the project team.

2.2 Determining Efficient Solutions

The first task in the Atana approach lies in determining efficient solution alternatives. Solving this problem that technically constitutes a multiobjective combinatorial optimization (MOCO; for a survey cf. [7]) problem involves the identification of Pareto-efficient combinations of controls in which the binary variables $x_i \in \{0,1\}$ indicate whether or not a control i is selected ($x_i = 1$ if so, and $x_i = 0$ otherwise).

A solution can be represented as vector $x = (x_1, \ldots, x_N)$, where N denotes the number of proposed controls or necessary choices between controls, respectively. The MOCO problem comprises the maximization of K objectives (such as costs, availability or usability)

$$\text{maximize} \quad u_k(x) \qquad \text{for } k = 1, \ldots, K. \tag{1}$$

Objective functions referring to criteria that should naturally be minimized (e.g., costs) can easily be transformed by simply multiplying the underlying objective values with (-1). The functions $u_k(x)$ may take any form (linear, non-linear, etc.) as long as they are defined for all (feasible) alternatives x. Note, that finding proper functions for criteria such as the expected availability of a given combination of controls may prove challenging, but this difficulty also holds true to the same degree for all other decision support approaches.

All solutions taken into consideration must be feasible with respect to two sets of constraints. The first set comprises limited resources (e.g., initial costs or running costs). For binary variables x_i constraints may be formulated simply as

$$\sum_i r_{iq} x_i \leq R_q \qquad \text{for } q = 1, \ldots, Q, \tag{2}$$

where r_{iq} represents the amount of resources of type q required by countermeasure i and R_q stands for the maximum available amount of resources. Corresponding terms must be added in the event of synergy or cannibalism effects that influence the total resource consumption. The second set ensures that at most a maximum – or at least a minimum – number of countermeasures from given subsets is included in the set of feasible solutions. For instance, a constraint may require that at least two defined countermeasures (referring to the corresponding countermeasures having assigned indices 1 to 6) but not more than four countermeasures must be selected and, thus, takes the form

$$2 \leq \sum_{i=1}^{6} x_i \leq 4. \tag{3}$$

Accordingly, decision makers can define that certain countermeasures should only be selected in combination with each other (e.g., the standard demands the combined use of a Security Guard and an Access System) and/or they can take into consideration that their combination yields synergy effects (e.g., the use of two countermeasures from the same vendor might result in reduced costs). Other countermeasures are mutually exclusive (e.g., countermeasures that provide exactly the same functionality) or cause cannibalism effects. For example, the use of a countermeasure fulfilling only part of the needed functionality might demand the use of a second countermeasure and thus would result in higher costs or reduced performance (cf. [23]).

2.3 Interactive Exploration of Solution Space

In Atana's second phase, the decision maker is supported in making a final determination of the solution that best fits his/her notions out of the possibly hundreds (or even thousands) of Pareto-efficient alternatives identified in the first phase. As we are using search-based procedures, we start from an efficient portfolio and allow the decision maker to iteratively "move" around in solution space towards more attractive alternatives until no better portfolio can be found (cf. an application by Focke and Stummer [11]). The Atana approach is based on interactive modifications of lower and upper bounds for one or more objectives. The decision support system (DSS) starts with displaying K "flying" bars (cf. Fig. 2).

For each objective (cf. Fig. 4) the system provides information on what can be achieved by (i) the efficient solutions (the corresponding marks may visually grow together to vertical blocks), and (ii) the alternatives that have remained after the decision makers have made decisions in their interactive exploration of the solution space.

Two moveable horizontal lines with small arrows at one side represent lower and upper bounds and are intended to restrict the set of remaining solutions in a step-by-step manner (e.g., by raising the minimum bound in one of the objectives) or for

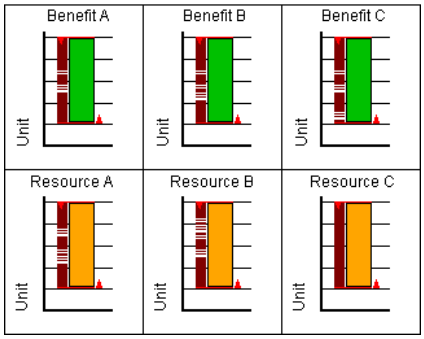

Fig. 2: Status of the DSS at the beginning

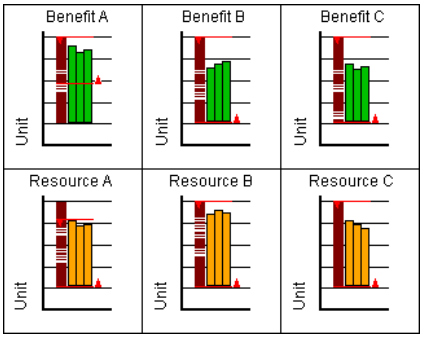

Fig. 3: Status of the DSS after two settings

expanding it (e.g., by once again relaxing some bounds) according to the decision makers' preferences. In all of these cases, the system provides immediate feedback about the consequences of such choices in terms of the remaining alternatives.

First the maximum allowance for resource A is reduced. Because this setting has primarily filtered those solutions that come with a relatively high value in "Resource Category A" (and, on average, a somewhat higher need for resource C) but still values in "Benefit Category A", the options in the other objectives have been reduced as well and the position and size of the flying bars have changed accordingly. Raising the minimum value for Benefit A (e.g., functionality) narrows the set of remaining alternatives even further, since many alternatives with low resource values (e.g., price) drop out (cf. Fig. 3).

In further iterations, the decision maker continues playing with minimum and maximum bounds and by doing so can learn about the consequences of his/her decisions and, thus, gain a much better "feeling" for the problem in terms of what can be achieved in some objectives at what "price" in terms of opportunity costs in other objectives. After several cycles of restricting and once again expanding the opportu-

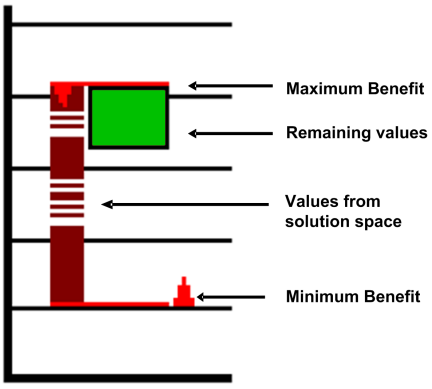

Fig. 4 Subwindow details

nity set, the decision maker will finally end up with a solution alternative that offers an individually satisfying compromise between the relevant objectives. The decision makers do not need to explicitly specify (i) weights for objectives, (ii) the form of their preference function or (iii) how much one solution is better than another during any stage of the whole procedure. Instead, the system provides ample information on the specific selection problem while it ensures that the final solution will be an optimal (i.e., Pareto-efficient) one, with no other feasible solution available that is better from an objective point of view.

3 Case Study

The case study was carried out in the social security sector in Austria. The goal of the organization was to obtain an ISO 27001 certification to comply to legal regulations and to further improve their commercial acceptance within the very sensitive social security sector. Therefore, we aimed at supporting the certification process by supporting decision makers in selecting Pareto-efficient implementation portfolios, which fulfill those ISO 27001 controls which require physical countermeasure implementations (e.g., ISO 27001 A.9.1.4 Control: Protecting against external and environmental threats). As described in Section 2, the security ontology splits all ISO 27001 controls into more granular controls, which are equipped with concrete implementation requirements that are necessary to fulfill the corresponding control. Figure 5 shows an example for ISO 27001 control A.9.1.1 and A.9.1.4 and the corresponding security ontology controls.

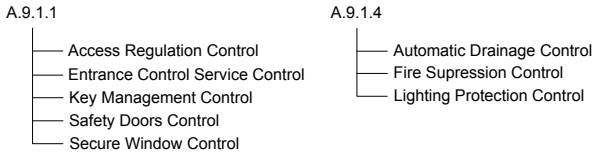

Fig. 5: ISO 27001 control A.9.1.1 and A.9.1.4

Splitting up the abstract ISO 27001 controls into more granular controls enables the definition of concrete implementation requirements. Figure 6 exemplarily shows the implementation requirements for the *Access Regulation Control*.

To fulfill the control the organization has to implement one access system (X1, X2, X3, or X4) and either one security guard (Sec Guard 1, Sec Guard 2, or Sec Guard 3) or one entry checkpoint (Ent Check 1, Ent Check 2, or Ent Check 3) at all entrances which connect sensitive to non-sensitive areas (e.g., main entrance of the building). Naturally only implementations should be contained in the final portfolio that support a successful certification and, thus, provide a strategic value for the company.

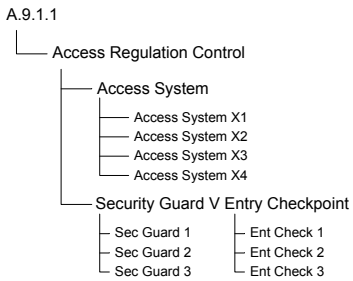

Fig. 6 Access Regulation Control implementation

3.1 Elicitation of Criteria

The criteria set defined in this section serves as main measurement objective for the evaluation of the investment candidates. Due to the multicriterial nature of our approach, a set of criteria is needed that is in line with the strategic objectives of the company. The primary goal of the company under consideration is to pass the certification process (achieved by considering the dependencies defined in section 3.2). At the same time, the company aims to implement measures that optimally cover the need for protection and are cost-efficient. Therefore, the criteria set includes financial criteria and security related objectives taken from literature (cf. [2]):

- Effectiveness (cf. [6]) is defined as the ability to achieve stated goals or objectives, judged in terms of both output and impact. Although our potential countermeasure implementations are not directly related to a specific threat (i.e., defined goals or objectives are missing), their effectiveness can be rated based on their primary purpose. For example, the main purpose of a fire detector is to detect fire and so we rate its effectiveness based on its ability to detect fire. At the current stage of research we are not considering side-effects of countermeasures (e.g., a security guard's primary purpose is to prevent unauthorized access but he would be also able to detect fire).
- Maintainability is a characteristic of design and installation, expressed as the probability that an item will be retained in or restored to a specified condition within a given period of time, when the maintenance is performed in accordance with prescribed procedures and resources [1].
- Reliability is defined by IEEE as the ability of a system or component to perform its required functions under stated conditions for a specified period of time (from 0 up to t). $R(t) = 1 - F(t)$ is the distribution function of the time to the first malfunction. $F(t) = exp(-t/T)$ in the case of an exponentially distributed time to malfunction, where parameter T defines the mean time to malfunction.
- The term running costs $q_{rc}(i)$ should be self-explanatory. They either depend on the maintenance costs or the number of requests.
- Finally, the initial costs $q_{ic}(i)$ represent the amount of money an enterprise has to invest in order to integrate a countermeasure i into its corporate environment.

An in-depth analysis then led to the criteria set summarized in Table 1. Note that depending on whether criteria can be measured in "real units" (e.g., monetary units, time units or measurable resource consumption), different scales are applied. If a category can be measured using a discrete number that relates to a real unit, investment candidates are assigned their absolute value. Otherwise (i.e., in case of intangible assets such as *Maintainability*), an abstract scale of *points* that ranges from 0 to 10 is used. Further note that each criteria is either of type *benefit* or if type *resource*, depending on whether the portfolios' category values should be maximized or minimized.

Code	Description	Unit	Limit
EF	Effectiveness	Pts.	Benefit
MA	Maintainability	Pts.	Benefit
RE	Reliability	Pts.	Benefit
IC	Initial Costs	€1,000	Resource
RC	Running Costs	€1,000	Resource

Table 1: Final set of objectives (selection criteria)

3.2 Definition of Investment Candidates

Prior to evaluating investment candidates, a set of feasible candidates is pre-selected from the ontological database. This selection is conducted by considering existing components and by performing a rough selection of potential investment candidates and comparing their main characteristics to the decision situation's base line parameters (knock-out criteria), such as available monetary or performance parameters. The number of investment candidates to include in individual evaluation strongly depends on several factors, including application domain and dependencies among the investment candidates – in this specific case, 26 candidates are selected. According to these preconditions and the requirements of the given certification controls, the components chosen for further evaluation are denoted with the letters A to Z and divided into ten groups: Access System (A, B, C, D), Security Guard (E, F, G), Entry Checkpoint (H, I, J), Safety Door (K, L, M), Acrylic Window (N, O), Security Film Window (P, Q), Tempered Window (R, S), Automatic Drainage System (T, U), Fire Extinguisher (V, W, X), and Lighting Arrester (Y, Z). Investment Candidates are rated based on data taken from the security ontology which incorporates specifications, empirical evaluations or estimations (cf. Table 2 for the rating of all investment candidates). Note that the ranges of the ratings differ depending on whether values naturally can be measured quantitatively (e.g., monetary units, time units or resource consumption). If so, investment candidates are directly assigned their absolute values for this criterion. Otherwise, an abstract scale of points is applied.

Candidate	EF	MA	RE	IC	RC
Access System					
Candidate A	2	9	2	9	5
Candidate B	7	9	9	1	7
Candidate C	0	1	6	6	7
Candidate D	0	1	3	17	34
Security Guard					
Candidate E	3	0	8	15	145
Candidate F	2	6	2	0	93
Candidate G	9	6	5	28	56
Entry Checkpoint					
Candidate H	5	3	3	7	12
Candidate I	0	0	9	4	6
Candidate J	5	1	10	27	55
Safety Door					
Candidate K	8	5	6	4	24
Candidate L	6	9	2	9	2
Candidate M	3	2	3	26	82
Acrylic Window					
Candidate N	0	3	6	23	45
Candidate O	2	6	8	1	120
Security Film Window					
Candidate P	9	1	1	9	71
Candidate Q	1	1	7	19	68
Wired Window					
Candidate R	10	4	8	29	26
Candidate S	9	7	7	11	49
Automatic Drainage System					
Candidate T	3	0	3	9	43
Candidate U	2	2	2	32	84
Fire Extinguisher					
Candidate V	8	6	6	20	40
Candidate W	10	2	7	2	22
Candidate X	2	5	8	2	9
Lighting Arrester					
Candidate Y	5	8	2	8	49
Candidate Z	2	6	3	40	70

Table 2: Ratings of investment candidates

3.3 Definition of Dependencies

Some (combinations of) decision alternatives entail dependencies. The ontological database provided the following interdependencies that we used as input for our interactive selection approach:

- **Access Regulation Control**
  $\forall$ *sec:implementedBy only*
  (ent:SecurityGuard $\vee$ *ent:AccessSystem* $\vee$ *ent:EntryCheckpoint)*;
  $\exists$ *sec:implementedBy some ent:AccessSystem*;
  $\exists$ *sec:implementedBy some (ent:SecurityGuard* $\vee$ *ent:EntryCheckpoint)*;
  in other words: the control is fulfilled if an access system or either an entry checkpoint or a security guard is in place.
- **Entrance Control Service Control**
  $\forall$ *sec:implementedBy only (ent:SecurityGuard* $\vee$ *ent:EntryCheckpoint)*;
  $\exists$ *sec:implementedBy some (ent:SecurityGuard* $\vee$ *ent:EntryCheckpoint)*;
  in other words: the control is fulfilled if either an entry checkpoint or a security guard is in place.
- **Safety Doors Control**
  $\forall$ *sec:implementedBy only ent:SafetyDoor*;
  $\exists$ *sec:implementedBy some ent:SafetyDoor*;
  in other words: the control is fulfilled if a safety door is in place.
- **Secure Window Control**
  $\forall$ *sec:implementedBy only*
  (ent:WiredWindow $\vee$ *ent:AcrylicWindow* $\vee$ *ent:SecurityFilmWindow)*;
  $\exists$ *sec:implementedBy some*
  (ent:WiredWindow $\vee$ *ent:AcrylicWindow* $\vee$ *ent:SecurityFilmWindow)*;

in other words: the control is fulfilled if either a wired window, a acrylic window, or a security film window is in place.

- **Automatic Drainage Control**
  ∀ *sec:implementedBy only ent:AutomaticDrainageSystem*;
  ∃ *sec:implementedBy some ent:AutomaticDrainageSystem*;
  in other words: the control is fulfilled if an automatic drainage system is in place.
- **Fire Supression Control**
  ∀ *sec:implementedBy only ent:FireExtinguisher*;
  ∃ *sec:implementedBy some ent:FireExtinguisher*;
  in other words: the control is fulfilled if a fire extinguishing system is in place.
- **Lighting Protection Control**
  ∀ *sec:implementedBy only ent:LightningArrester*;
  ∃ *sec:implementedBy some ent:LightningArrester*;
  in other words: the control is fulfilled if a lighting arrester is in place.

3.4 Interactive Selection of ISO 27001 Controls

Following the multiobjective decision support procedure described in section 2.2, the process starts by importing the categories together with potential controls and dependencies from the ontology. Depending on the number of objectives, constraints and business processes, Atana is capable of evaluating about 40 investment candidates per decision situation. In our case study (which includes five objectives plus 26 investment candidates) the underlying MOCO problem can be solved on an average workstation in less than one minute. Thus, 249 non-dominated (i.e., Pareto-efficient) feasible portfolios are identified. These solution alternatives are further evaluated using Atana's interactive decision support module.

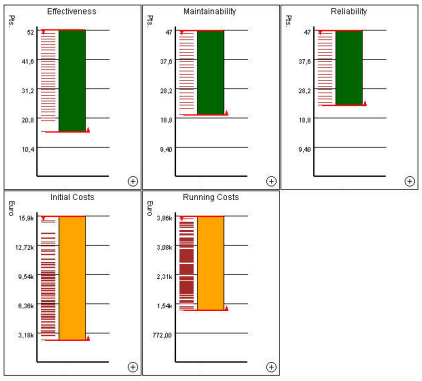

Fig. 7 Initial mask of the Atana analysis tool

Figure 7 shows the initial screen of the analysis tool. By moving the red upper and lower rulers, aspiration levels are set (for minimum or maximum values in a given

objective category) and, thus, the number of remaining solutions can be reduced in a straightforward manner. In our example, this is performed as follows: at first, the maximum initial costs are reduced to a value of 6k and the running costs to a level of 2k, which reduces the number of portfolios from 249 to 23 (cf. Fig. 8).

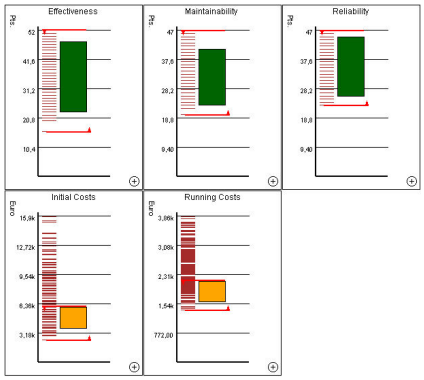

Fig. 8: Mask after the user's first setting

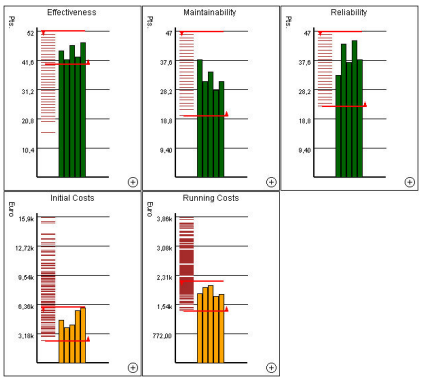

Fig. 9: Mask after the user's final setting

After this, the minimum requirement for effectiveness is set to a value of 40 points, while the corresponding values for maintainability and for reliability remain unchanged. Afterwards, the remaining five portfolios are visualized side by side (cf. Fig. 9). The remaining portfolios (cf. Table 3) provide benefits on an average level

Portfolio	Controls	EF	MA	RE	IC	RC
1	B, H, L, S, T, W, Y	45	38	33	4700	1800
2	B, I, K, S, T, W, Y	42	31	43	3900	2000
3	B, H, K, S, T, W, Y	47	34	37	4200	2060
4	B, I, K, R, T, W, Y	43	28	44	5700	1770
5	B, H, K, R, T, W, Y	48	31	38	6000	1830

Table 3: List of the remaining portfolios

and are associated with average resource consumptions. Note that the second and fourth portfolio provide the highest values for reliability, but also the lowest values for effectiveness and maintainability. Portfolios two and three come with the lowest initial costs but have the highest running costs of all solutions, whereas their benefits are on an average level. Depending on the decision makers preferences, one of these can either be selected or the evaluation process can be continued by picking other portfolios and/or (re-)setting the aspiration levels.

4 Conclusions and Further Work

Although an organization benefits from an information security certification in several ways, most companies refrain from the implementation of information security standards, amongst other reasons due to the lack of methods for measuring the cost/benefits ratio of potential countermeasure implementations. In this paper we proposed a new two-phase approach, which supports decision makers in defining the optimal set of countermeasures complying to the ISO 27001 standard. In the first step, the security ontology serves as an ontological knowledge base for potential countermeasure implementations (and combinations thereof), which are required to obtain an ISO 27001 certification. In the second step, the decision support system Atana determines solution alternatives that are both feasible with respect to given constraints and Pareto-efficient with respect to multiple objectives. Thereby we give decision makers an instrument that allows them to interactively select tangible countermeasures based on the abstract descriptions of controls from security standards such as ISO 27001. In the case study we showed how Atana supports decision makers in interactively exploring the determined solution space to find their individually "best" solution. While this paper addresses mainly physical countermeasure implementations (e.g., fire extinguisher, secure windows, or safety doors), further research activities will address the inclusion of organizational aspects (e.g., policy components, legal regulations) to support the ISO 27001 certification in the most holistic way. We will also consider the dependencies among countermeasures and vulnerabilities to ensure that potential countermeasure side-effects are regarded within the Atana methodology.

Acknowledgements This work was performed at Secure Business Austria, a competence center that is funded by the Austrian Federal Ministry of Economics and Labor (BMWA) as well as by the provincial government of Vienna.

References

1. Federal standard 1037c. URL http://www.its.bldrdoc.gov/fs-1037/fs-1037c.htm, last access: 7 April 2008
2. Avizienis, A., Laprie, J.C., Randell, B., Landwehr, C.: Basic Concepts and Taxonomy of Dependable and Secure Computing. IEEE Transactions on Dependable and Secure Computing **1**(1), 11–33 (2004)
3. BASEL2: Basel Committee on Banking Supervision (BCBS), Basel 2 - International Convergence of Capital Measurement and Capital Standards - A Revised Framework (2001)
4. British Department of Trade and Industry (DTI): BS7799-2:2002 Information security management systems - Specification with guidance for use (2002)
5. BSI: IT Grundschutz Manual. Online: http://www.bsi.bund.de/gshb/ (2004).
6. Bureau of Justice Assistance: Center for Program Evaluation - Glossary. Online: http://www.ojp.usdoj.gov/BJA/evaluation/glossary/glossary_e.htm, last access: 7 April 2008 (2007)

7. Ehrgott, M., Gandibleux, X.: A survey and annotated bibliography of multiobjective combinatorial optimization. OR Spectrum **22**(4), 425–460 (2000)
8. Ekelhart, A., Fenz, S., Klemen, M., Weippl, E.: Security Ontology: Simulating Threats to Corporate Assets. In: A. Bagchi, V. Atluri (eds.) Second International Conference, ICISS 2006, December 19-21, *Lecture Notes in Computer Science*, vol. 4332/2006, pp. 249–259. Springer Berlin / Heidelberg, Kolkata, India (2006). DOI 10.1007/11961635_17
9. Ekelhart, A., Fenz, S., Klemen, M., Weippl, E.: Security ontologies: Improving quantitative risk analysis. In: 40th Hawaii International Conference on System Sciences (HICSS'07), pp. 156–162. IEEE Computer Society, Los Alamitos, CA, USA (2007).
10. Fenz, S., Goluch, G., Ekelhart, A., Riedl, B., Weippl, E.: Information security fortification by ontological mapping of the ISO/IEC 27001 Standard pp. 381–388 (2007).
11. Focke, A., Stummer, C.: Strategic technology planning in hospital management. OR Spectrum **25**(2), 161–182 (2003)
12. Gordon, L., Loeb, M., Lucyshyn, W., Richardson, R.: 2006 CSI/FBI Computer Crime and Security Survey (2006)
13. Gruber, T.: A translation approach to portable ontology specifications. Knowledge Acquisition **5**(2), 199–220 (1993).
14. International Organization for Standardization and International Electrotechnical Commission: ISO/IEC 17799:2005, information technology – code of practice for information security management (2005)
15. International Organization for Standardization and International Electrotechnical Commission: ISO/IEC 27001:2005, information technology - security techniques - information security management systems- requirements (2005)
16. Ittner, C.D., Larcker, D.F.: Coming Up Short On Financial Measurement. Harvard Business Review **81**(11), 88–95 (2003)
17. Neubauer, T., Stummer, C.: Extending business process management to determine efficient IT investments. In: Proceedings of the 2007 ACM Symposium on Applied Computing, pp. 1250–1256 (2007)
18. Neubauer, T., Stummer, C.: Interactive decision support for multiobjective cots selection. In: Proceedings of the 40th Annual Hawaii International Conference on System Sciences, 01 (2007)
19. Neubauer, T., Stummer, C., Weippl, E.: Workshop-based Multiobjective Security Safeguard Selection. In: Proceedings of the First International Conference on Availability, Reliability and Security ARES, pp. 366–373. IEEE Computer Society (2006)
20. NIST: An introduction to computer security - the nist handbook. Tech. rep., NIST(National Institute of Standards and Technology) (1995). URL http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf. Special Publication 800-12
21. PriceWaterhouseCoopers: Information Security Breaches Survey. www.dti.gov.uk/industries/information_security, last access: 7 April 2008 (2006)
22. SOX: One hundred seventh congress of the United States of America, Sarbanes Oxley Act - to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes. (2002)
23. Stummer, C., Heidenberger, K.: Interactive R&D portfolio analysis with project interdependencies and time profiles of multiple objectives. IEEE Transactions on Engineering Management **50**(2), 175–183 (2003)
24. World Wide Web Consortium: OWL - Web Ontology Language. http://www.w3.org/TR/owl-features/, last access: 7 April 2008 (2004)