An Answer Set Solution for Information Security Management

Carlos Cares, Mauricio Diéguez

Computer Science and Informatics Department,
University of La Frontera (UFRO)
Temuco, Chile
Email: {carlos.cares,mauricio.dieguez}@ceisufro.cl

***Abstract*—Information Security Management is focused on processes and it is currently guided by control-based standards such as ISO27002. Controls may be: management objectives, available resources or desired behaviours that contribute to information security. Under this process perspective, to reach some security level means to accomplish a specific set of controls. There are qualitative approaches and maturity models that help managers to select what controls to implement next, whilst quantitative approaches have just recently emerged under simplified formulations. The purpose of this paper is to show an answer set solution to the problem of selecting what controls to implement next, based on a given budget, security profit, and temporal dependencies between controls. The solution is illustrated by using Clingo.**

Keywords–Information security; Controls selection; Answer set programming; Clingo.

I. INTRODUCTION

A standard for information security consists of a set of rules that aim to regulate a company's operation, with a special emphasis on information management and information assurance. In general, the accomplishment of some information security standard means to achieve a set of objectives, get resources or implement actions defined by the standards [1]. All these elements are known as information security controls [2] and may be grouped by dimensions.

In particular, one of the most widely-known security standards is ISO/IEC 27001:2013 [3]. This standard proposes 114 controls classified in 14 main dimensions, described in ISO/IEC 27002:2013 [4]. The degree of compliance with these controls determines the organization's security level and whether it can apply for certification.

Therefore, the map of implemented/non-implemented controls becomes a management tool to progress in information security. In Table I, some examples of controls and their corresponding dimensions from ISO27002 are shown.

TABLE I. EXAMPLES OF INFORMATION SECURITY CONTROLS AND DIMENSIONS FROM ISO27002.

Domain: Information security policies
Policies for information security
Review of the policies for information security
Domain: Human resource security
Terms and conditions of employment
Information security awareness, education and training
Domain: Cryptography
Policy on the use of cryptographic controls
Key Management
Domain: Physical and environmental security
Physical security perimeter
Equipment maintenance
Domain: Operations security
Documented operating procedures
Information backup
Domain: Compliance
Protection of records
Technical compliance review

The general problem of managing information security has been addressed through different approaches and different disciplines [5]–[7]. Various frameworks have been proposed for measuring the level of standard compliance [8]–[11]; however, these approaches do not suggest a plan for the implementation of controls, obtained quantitatively from the current level of compliance to some desired security level.

Investigations in this area have led to the incorporation of quantitative methods for managing security controls, some of them based on multicriteria analysis, such as, [12]–[14]. Other investigations [15]–[21], combined the System Grey Theory [22] with other quantitative techniques of analysis.

Another investigation proposed a simulation-based approach [23]–[25]. In this approach, simulated attacks are run over a model of the organization. Each attack occurs under different scenarios of implemented controls. According to the results of the simulations, the optimal set of controls is determined. The difficulty of this method is that choosing different sets of controls to simulate an attack is a human task within a combinatorial framework.

It seems clear that optimizing controls implementations is an open problem where quantitative approaches are just emerging. In [26] ,the conceptual framework for a quantitative optimization approach and several types of constraints are described. Mainly, we remark the temporal dependency between controls, the existence of a given budget, and the objective function focused on maximizing security by minimizing vulnerabilities.

To solve this quantitative optimization problem, we propose an answer set solution approach. Answer set programming is a research product on knowledge representation, logic programming and constraint satisfaction to cope mainly with np-hard problems [27]. Nowadays, there are some mature tools allowing the specification and solution of general models [28].

In this paper, we propose a specific solution approach for selecting controls by using the answer set tool named Clingo [29]. Clingo is a framework to solve combinatorial problems with Answer Set Programming (ASP), a simple and powerful modeling language [30].

In order to show the solution, in section II, we explain

 ISBN: 978-1-61208-535-7

the basis of the model by means of a small, but illustrative example. In section III, we show the results of applying the model using data from a public governmental office. The conclusion section highlights the simplicity of the proposed model but also the necessity to compare this approach to traditional models from operational research.

II. ANSWER SET MODELLING FOR SELECTING SECURITY CONTROLS

The basic principle to be applicable in an answer set solution is that there are different possible solutions, i.e., there is a space of solutions to be evaluated. An answer set program may be composed of four sections: (i) the first section expressing the basic configuration of the problem, (ii) the second section for generating the different answer sets, (iii) the third section for the derived or non basic definitions plus the terms to evaluate solutions, and (iv) the fourth section containing the problem constraints. These forms are briefly reviewed.

The basic configuration is composed of true facts, which are represented as literals (classic propositions) or predicates on specific literals (objects). The possible forms are as follows:

$$\begin{aligned} &l_0. \\ &P_1(l_1). \\ &P_2(l_2, l_3). \end{aligned} \tag{1}$$

To represent the different answer sets, rules are needed. These rules are known as the disjunctive form because several alternatives, represented as a set, may be generated starting from proved facts. These rules have the following form:

$$\mathrm{l}\{\mathrm{A}_0, A_1, ..., A_k\}\ u \leftarrow\ A_1, ..., A_n. \tag{2}$$

Under this form, the alternatives in the set stay bound by l and u, and these values represent the minimum and maximum number of elements in the set, provided, of course, that it is possible to derive them from the true conjuctions A_1 to A_n.

The third section should represent the definitions in the universe of discourse. In this case, the rules follow a simplified version of the previous form, this time without alternative sets, i.e., having only predicates on variables or literals in the left part. Thus, classical definitions may have the following form:

$$\begin{aligned} P_0(V_0) &\leftarrow\ A_1, A_2, ... \\ P_1(V_1, V_2) &\leftarrow B_1, B_2, ... \end{aligned} \tag{3}$$

The fourth section specifies the constraints. These are specified similar to the previous rules, but having only the right part, as follows:

$$\leftarrow A_0, A_1, ..., A_n. \tag{4}$$

In order to illustrate the given solution, we consider an example having ten controls, a set of temporal dependencies, and each control having its corresponding implementation cost and also a corresponding security profit. In Fig. 1, we show the basic configuration of the example. First, we have the identification of the control (C1 to C10), its cost and profit (third value). This security profit is abstract and may be considered from a single increment in the percentage of a standard accomplishment, to the reduction of vulnerabilities belonging to key information assets. The dependencies are represented by the curly brackets. For example, the control C5 may be implemented if and only if controls C1 and C2 have been already implemented.

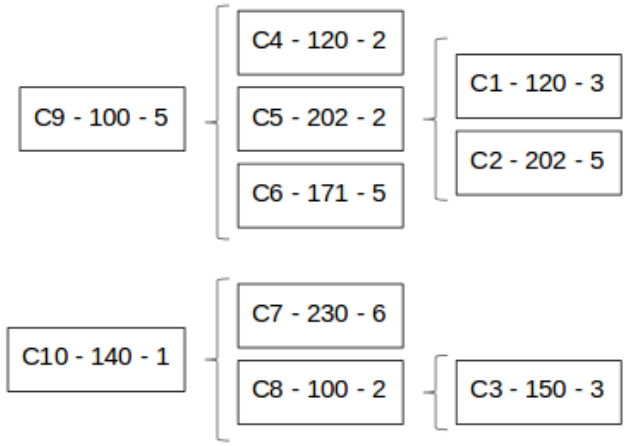

Figure 1. Candidate controls to implement, their cost, profit and dependencies.

Firstly, we notice that there are several possible answers that match the answer set conditions to be applied, under a bounded budget. For example, for a given budget of 500, we may have an implementation plan including the controls C3, C8 and C10, having a total cost of 390 (150+100+140) and a total profit of 6 (3+2+1). But also we may have an implementation plan including the controls C1, C2 and C6 having a total cost of 492 and a total profit of 11.

In order to code the solution, we have used Clingo 4.5.4 [29]. As described above, we divide the explanation in four parts.

To configure the basic initial state, we have used the predicates: *control*, for setting the variables that represent controls, *cost*, for specifying the implementation cost of each control, and *require*, for representing the dependencies between controls. In Fig. 2, we show the Clingo sentences for this configuration.

```
control(c1;c2;c3;c4;c5;c6;c7;c8;c9;c10).

cost(c1,200).
cost(c2,301).
cost(c3,150).
%  ...
profit(c1,3).
profit(c2,5).
profit(c3,3).
%...
require(c9,(c4;c5;c6)).
require(c5,(c1;c2)).
require(c10,(c7;c8)).
require(c8,c3).
```

Figure 2. Partial configuration of current state.

 ISBN: 978-1-61208-535-7

To represent the answer sets, we have used two rules that we show in Fig. 3. The first rule represents that it is possible to plan a specific control (variable Y) provided that this control does not depend on other controls. The bounds 0 and 1 specify that this control may or may not be part of the solution. The second rule states that a control that depend on others can also be part of the solution, provided that all their required controls (*totalRequired*) have been planned (*totalIncluded*).

```
%Generate
0 { planned(Y) } 1
    :- terminal(Y).
0 { planned(X) } 1
    :- totalRequired(X,D) ,
       totalIncluded(X,W), D==W.
```

Figure 3. Rules generation.

The necessary definitions are in Fig. 4. Here, we define the formulas for total cost, total profit, total number of required controls for each control, and total number of planned controls among the required ones. Finally, we show the definition of terminal controls that are defined as those controls that do not require the implementation of previous controls in order to plan them.

```
%Define
totalRequired(X,D):-
    control(X),
    D = #count {Z: require(X,Z),
                   control(Z)}.
totalIncluded(X,D):-
    control(X),
    D = #count {Z: require(X,Z),
                   planned(Z)}.
totalProfit(Y):-
    Y = #sum {D,X: planned(X),
                   profit(X,D)}.
totalCost(N) :-
    N = #sum {D,X: planned(X),
                   cost(X,D)}.
terminal(X):-
   control(X),
   not require(X,_).
```

Figure 4. Definitions.

Finally, the fourth section is shown in Fig. 5. This contains the definition of the available budget and the constraint that the total cost needs to always be less than the budget. Moreover, Clingo allows to add optimization expressions by using the macro clauses *maximize* or *minimize*. In this case, we have used *maximize* to search for the best result on information security profit (*totalProfit*). In Fig. 6, the result is illustrated, as displayed by Clingo. For the given example, the solution included the controls C1, C3, C4, C6 and C7, having a total cost of 871 and a total profit of 19.

Finally, we present Table II, to illustrate the combinatorial power of this problem, under the given constraints.

```
%Test
budget(900).
:- totalCost(N),
   budget(T),
   N>T.

%Optimization
#maximize
   { I:totalProfit(I) }.
```

Figure 5. Constraints and Optimization.

```
clingo version 4.5.4
Reading from sms.lp
Solving...
Answer: 1
totalProfit(0) totalCost(0)
Optimization: 595
Answer: 2
planned(c3) totalProfit(3) totalCost(150)
Optimization: 592
Answer: 3
planned(c3) planned(c7) totalProfit(9) totalCost(380)
Optimization: 586
Answer: 4
planned(c1) planned(c3) planned(c7) totalProfit(12) total
Cost(580)
Optimization: 583
Answer: 5
planned(c1) planned(c2) planned(c3) planned(c7) totalProf
it(17) totalCost(881)
Optimization: 578
Answer: 6
planned(c1) planned(c3) planned(c4) planned(c6) planned(c
7) totalProfit(19) totalCost(871)
Optimization: 576
OPTIMUM FOUND

Models       : 6
  Optimum    : yes
Optimization : 576
Calls        : 1
Time         : 0.116s (Solving: 0.03s 1st Model: 0.00s Un
sat: 0.02s)
CPU Time     : 0.120s
```

Figure 6. Candidate controls to implement, their cost, profit and dependencies.

TABLE II. NUMBER OF POSSIBLE ANSWER SETS BY BUDGET.

Budget	Answer sets
2000	147
1500	144
1000	103
900	87
700	57

In this table, we summarize, a what-if analysis for the current example showing the total of possible answer sets given by different budgets.It is possible to get them running Clingo with the option -n 0.

III. EXAMPLE

To illustrate the operation of the proposal in a real situation, we have applied the proposed model to a situation adapted from a real audit of a public organization of the Chilean State. The proposal must recommend the optimal set of controls to

be implemented, considering a limited budget, the costs of implementing the controls and the benefits obtained by the progress in complying with the controls of the standard.

In this case, the organization wished to evaluate its compliance with three standards of information security to which it subscribed. As a public entity, the organization must comply with the information security regulations established by the Government of Chile: (i) Supreme Decree 83 (DS83) [31], a security standard for public offices; and (ii) the methodological guide for information security (GUI) [32], in the framework of the Chilean government's improvement program, which describes the technical requirements associated with the diagnosis, planning and implementation of an information security system. In addition, the organization decided to evaluate its compliance with the international ISO Standard 27001, in its 2005 version.

For the purposes of the example, we will only present the dimension referring to the security of facilities, since it was the main focus of evaluation after the earthquake of the year 2010 in Chile. In this dimension, we analyzed 30 controls from the three above standards.

The benefits associated to each control were established considering the standard to which they belong to. We represent greater benefits on those controls explicitly mentioned into the Chilean norms of information security for public institutions. Therefore, those controls, that belong to more than one standard, will report a greater benefit to the organization. Considering this, a higher score was given to the controls that met the rules of the government of Chile and those that satisfied more than one norm.

The implementation costs of each control were estimated based on the operating conditions of the organization. In addition, a budget constraint was assigned to the problem.

In this way, the model delivers the set of controls that, considering costs and budget, provides the higher benefit to the organization. The implementation of the situation yielded 18 possible responses to the problem, which met the constraints of the problem. Table III, summarizes the progress of the optimization process. The table shows the number of implemented controls (second column), their corresponding cost (third column) and the previewed benefit (fourth column).

It should be noted that the 18 delivered answers do not correspond to the total universe of possible solutions. The implementation only shows those sets of controls that present a better profit than the previous answers. Therefore, the last line represents the final recommendation which includes a set of 22 controls that reports a benefit of 55 at a cost of $ 19.950.000 (expressed in Chilean money).

The model, i.e. predicates, rules, and constraints of this case example can be downloaded from [33]

TABLE III. FEASIBLE ANSWERS IN THE CHILEAN PUBLIC CASE EXAMPLE.

Answer	Number of Controls	Total Cost	Total Profit
Answer 1	8	$ 11.360.000	21
Answer 2	9	$ 13.360.000	24
Answer 3	10	$ 16.360.000	27
Answer 4	11	$ 17.160.000	30
Answer 5	12	$ 19.960.000	34
Answer 6	14	$ 17.800.000	37
Answer 7	15	$ 18.600.000	38
Answer 8	15	$ 18.500.000	41
Answer 9	16	$ 19.300.000	42
Answer 10	17	$ 19.700.000	43
Answer 11	16	$ 18.760.000	45
Answer 12	17	$ 19.160.000	46
Answer 13	18	$ 19.960.000	47
Answer 14	16	$ 19.720.000	49
Answer 15	21	$ 19.850.000	52
Answer 16	22	$ 19.750.000	53
Answer 17	21	$ 19.250.000	54
Answer 18	22	$ 19.950.000	55

IV. CONCLUSIONS

A contemporary approach to manage information security on organizations is following process-based standards as the family of norms ISO/IEC27000. This process recommends the implementation of a set of security controls (e.g. ISO/IEC27002). From this perspective, in order to accomplish the standard, an information security assessment produces, as relevant outcomes, a set of controls already implemented and another set of controls to implement. Making a decision about the next information security controls to implement is a np-hard problem. This has been demonstrated in [34] for the general problem of process-based compliance norms. Under this approach, the unique isomorphism to apply is to consider as separate tasks the implementation of security controls, which is what we have modeled in our answer set programming approach.

Although other quantitative solutions have been proposed, here we have presented a solution having three kinds of constraints: temporal dependencies between controls, a limited budget, and different information security profits given by the different controls to implement. Under the consideration of this set of different variables, as far as we know, it is the most complex quantitative solution shown in an academic setting.

We have shown an answer set programming solution simple and illustrative. Firstly, we have shown that a quantitative solution is not hard to implement, and, moreover, secondly, it can be easily extended to support additional controls (facts) and constraints, due to the modular nature of rules in answer set programming.

However, it is known that answer set solutions are based on general optimization settings. For this reason, it logically follows that specific operational research solutions may present a better performance. Therefore, in terms of future work, we will compare this answer set programming solution to classical optimization algorithms on operation research platforms, but we would like to add modelling time as a variable to observe.

ACKNOWLEDGMENT

The authors would like to thank DIUFRO project DI13-0068 from the Vice-rectory of Research and Development from University of La Frontera, by supporting different aspects of this work.

REFERENCES

[1] T. Pereira and H. Santos, "Challenges in information security protection," *Proceedings 13th European Conference on Cyber Warfare and Security*, pp. 160–166, 2014.

[2] H. Yau, "Information security controls," *Advances in Robotics & Automation*, vol. 3, no. 2, 2014, doi: 10.4172/2168-9695.1000e118.

[3] ISO/IEC27001. Information security management. [Online]. Available: http://www.iso.org/iso/home/standards/management-standards/iso27001.htm, [retrieved: January, 2017]

 ISBN: 978-1-61208-535-7

[4] ISO/IEC27002. Information technology – security techniques – code of practice for information security controls. [Online]. Available: http://www.iso.org/iso/catalogue_detail?csnumber=54533, [retrieved: January, 2017]

[5] M. Siponen and H. Oinas-Kukkonen, "A review of information security issues and respective research contributions," *ACM SIGMIS Database*, vol. 38, no. 1, pp. 60–80, 2007.

[6] K. Padayachee, "Taxonomy of compliant information security behavior," *Computers & Security*, vol. 31, no. 5, pp. 673–680, 2012, doi:10.1016/j.cose.2012.04.004.

[7] E. Kolkowska and G. Dhillon, "Organizational power and information security rule compliance," *Computers & Security*, vol. 33, pp. 3–11, 2013, doi:10.1016/j.cose.2012.07.001.

[8] T. Butler and D. McGovern, "A conceptual model and is framework for the design and adoption of environmental compliance management systems," *Information Systems Frontiers*, vol. 14, no. 2, pp. 221–235, 2009, doi:10.1007/s10796-009-9197-5.

[9] R. Bonazzi, L. Hussami, and Y. Pigneur, "Compliance management is becoming a major issue in is design," *Information Systems: People, Organizations, Institutions, and Technologies*, pp. 391–398, 2009, doi:10.1007/978-3-7908-2148-2_45.

[10] H. Susanto, M. Almunawar, and Y. Tuan, "Information security challenge and breaches: Novelty approach on measuring iso 27001 readiness level," *International Journal of Engineering and Technology*, vol. 2, no. 1, pp. 67–75, 2012, doi:10.1016/j.im.2008.12.007.

[11] M. Montanari, E. Chan, K. Larson, W. Yoo, and R. Campbell, "Distributed security policy conformance," *Computers & Security*, vol. 33, pp. 28–40, 2013, doi:10.1016/j.cose.2012.11.007.

[12] Y. Yang, H. Shieh, J. Leu, and G. Tzeng, "A vikor-based multiple criteria decision method for improving information security risk," *International journal of information technology & decision making*, vol. 8, no. 2, pp. 267–287, 2009, doi:10.1142/s0219622009003375.

[13] J. Lv, Y. Zhou, and Y. Wang, "A multi-criteria evaluation method of information security controls," *Fourth International Joint Conference on Computational Sciences and Optimization*, pp. 190–194, 2011, doi:10.1109/cso.2011.43.

[14] Y. Yang, H. Shieh, and G. Tzeng, "A vikor technique based on dematel and anp for information security risk control assessment," *Information Sciences*, vol. 232, pp. 482–500, 2013, doi:10.1016/j.ins.2011.09.012.

[15] L. Chen, L. Li, Y. Hu, and K. Lian, "Information security solution decision-making based on entropy weight and gray situation decision," *Fifth International Conference on Information Assurance and Security*, vol. 2, pp. 7–10, 2009, doi:10.1109/ias.2009.9.

[16] X. Cuihua and L. Jiajun, "An information system security evaluation model based on ahp and grap," *International Conference on Web Information Systems and Mining*, pp. 493–496, 2009, doi:10.1109/wism.2009.105.

[17] C. Yameng, S. Yulong, M. Jianfeng, C. Xining, and L. Yahui, "Ahp-grap based security evaluation method for mils system within cc framework," *Seventh International Conference on Computational Intelligence and Security*, 2011, doi:10.1109/cis.2011.145.

[18] J. Breier and L. Hudec, "New approach in information system security evaluation," *IEEE First AESS European Conference on Satellite Telecommunications (ESTEL)*, pp. 1–6, 2012, doi:10.1109/estel.2012.6400145.

[19] ——, "On selecting critical security controls," *International Conference on Availability, Reliability and Security*, pp. 582–588, 2013, doi:10.1109/ares.2013.77.

[20] ——, "On identifying proper security mechanisms," *Information and Communicatiaon Technology*, pp. 285–294, 2013, doi:10.1007/978-3-642-36818-9_29.

[21] J. Breier, "Security evaluation model based on the score of security mechanisms," *Information Sciences and Technologies Bulletin of the ACM*, vol. 6, no. 1, pp. 19–27, 2014.

[22] J. Deng, "Introduction to grey system theory," *The Journal of grey system*, vol. 1, no. 1, pp. 1–24, 1989.

[23] E. Kiesling, C. Strausss, and C. Stummer, "A multi-objective decision support framework for simulation-based security control selection," *Seventh International Conference on Availability, Reliability and Security*, pp. 454–462, 2012, doi:10.1109/ares.2012.70.

[24] E. Kiesling, A. Ekelhart, B. Grill, C. Straub, and C. Stummer, "Simulation-based optimization of it security controls: Initial experiences with meta-heuristic solution procedures," *in in 14th EUME Workshop*, 2013.

[25] E. Kiesling, C. Strauss, A. Ekelhart, B. Grill, and C. Stummer, "Simulation-based optimization of information security controls: An adversary-centric approach," *Winter Simulations Conference (WSC)*, 2013, doi:10.1109/wsc.2013.6721583.

[26] M. Diéguez, S. Sepúlveda, and C. Cares, "On optimizing the path to information security compliance," *Eighth International Conference on the Quality of Information and Communications Technology (QUATIC)*, pp. 182–185, 2012.

[27] G. Brewka, T. Eiter, and M. Truszczyński, "Answer set programming at a glance," *Communications of the ACM*, vol. 54, no. 12, pp. 92–103, 2011.

[28] M. Gebser and et al., "Potassco: The potsdam answer set solving collection," *Ai Communications*, vol. 24, no. 2, pp. 107–124, 2011.

[29] M. Gebser, R. Kaminski, B. Kaufmann, and T. Schaub, "Clingo= asp+ control: Preliminary report," *arXiv preprint arXiv:1405.3694*, 2014.

[30] M. Gebser, R. Kaminski, B. Kaufmann, M. Ostrowski, T. Schaub, and S. Thiele, "A user's guide to gringo, clasp, clingo, and iclingo," 2008.

[31] E. de Chile. Decreto 83: Norma técnica para los órganos de la administración del estado sobre seguridad y confidencialidad de los documentos electrónicos. Http://www.leychile.cl/Navegar?idNorma=234598, [retrieved: January, 2017].

[32] G. de Chile. Programa de mejoramiento de la gestión sistema de seguridad de la información: Versión 2011. Http://www.dipres.gob.cl/594/w3-propertyvalue-16887.html, [retrieved: January, 2017].

[33] C. Cares and M. Diéguez. Oscufro: Asp configuration for optimal security controls. Http:// dci.ufro.cl/ fileadmin/ Software/ OptimalSecurityControls-OSCUFRO.zip., [retrieved: January, 2017].

[34] S. C. Tosatto, G. Governatori, and P. Kelsen, "Business process regulatory compliance is hard," *IEEE Transactions on Services Computing*, vol. 8, no. 6, pp. 958–970, 2015.

 ISBN: 978-1-61208-535-7