TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies
Software Engineering Department

Kadri Cahani 165492

ALIGNING INFORMATION SECURITY RISKS WITH STRATEGIC GOALS

Master Thesis

Supervisor
Dr. Hayretdin Bahşi

Tallinn 2020

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Kadri Cahani 165492

INFOTURBE RISKIDE HINDAMINE LÄHTUVALT STRATEEGILISTEST EESMÄRKIDEST

Magistritöö

Juhendaja
Dr. Hayretdin Bahsi

Tallinn 2020

Author's declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Kadri Cahani .....
(signature)

Date: May, 16, 2020

Abstract

The prioritization of IT risks based on strategic goals, would enable information security teams into efficient resource allocation and this alignment would increase coordination and communication between information security team and decision makers. Focusing on the most crucial risks would save time and be an important step to preparing against security incidents.

The objective of this study is to prioritize risks according to the organisational strategic goal by using multi criteria decision making methods. This will consist of bringing in together information technology risks and strategic goals and in the end have a list of risks, prioritized not only from technology perspective, but also including objectives set by executive leadership. For areas that strategic goals and information technology risks concern, I propose linking them with domains proposed from ISO27001 standard by using Analytic Hierarchy Process (AHP) and Analytic Network Process (ANP) methods. ISO27001 is a widely used standard in information security while AHP and ANP are multiple criteria methods used to provide ranking of risks. In this thesis, I bring a use case about the proposed approach and by all means, using one organization is not sufficient and different types of organizations need to be tried out and reflect on end results. Results show that applying these methods help to differentiate risks among each other based on relationships created with domains, which from the other side reflect areas of interest for strategic goals.

This study should trigger more interest into how risk management is organized with regard to strategic goals of an organization and it simplifies the list of risks by differentiating them between each other. The novelty of it lies on using already collected information but bringing more clarity on telling risks apart from each other using a method for ranking.

The thesis is written in English and contains 54 pages of text, 6 chapters, 19 figures and 24 tables.

Annotatsioon

Infoturbe riskide hindamise, lähtuvalt strateegilistest eesmärkidest, prioriteetseks seadmine võimaldaks infoturbe spetsialistidel tõhusamalt asutuse ressursse kasutada ning seeläbi paraneks ka tööprotsessi koordineeritus ning infovahetus spetsialistide ja juhtkonna vahel. Olulisematele riskifaktoritele keskendudes on võimalik säästa aega ning olla paremini valmis võimalikeks infoturbe intsidentideks.

Antud uurimuse eesmärk on tutvustada multikriteeriumi otsustusmeetodit, mille abil saab tähtsusjärjestada riske, lähtudes seejuures organistatsiooni strateegilisest eesmärgist. See meetod toob ühte loendisse kokku infotehnoloogilised riskid ja strateegilised eesmärgid, mis on prioriteetses järjestuses mitte ainult tehnoloogia vaatevinklist, vaid sisaldades ka juhtkonna sihteesmärke. Need tegevussfäärid, mis nii strateegilisi eesmärke kui IT riske puudutavad, võiks minu hinnangul kokku koondada ISO27001 standarddomeeni, kasutades AHP ja ANP meetodeid. Küberturbe valdkonnas on ISO27001 standard laialdases kasutuses; AHP ja ANP on aga multikriteeriumi meetodid, mida rakendatakse riskifaktorite järjestamisel. Selles töös uurin ma antud meetodit ühe organisatsiooni näitel, kuid kindlasti pole see küllaldane põhjalikeks järeldusteks ning vajalik oleks uuringuid jätkata erinevat tüüpi organisatoorsetes keskkondades. Senised tulemused näitavad, et multikriteeriumi otsustusmeetod aitab riske diferentseerida, tuginedes domeenide vahelistele seostele, mis ühtlasi strateegilisi huve kajastavad.

Siinne uurimistöö võiks ärgitada rohkem huvituma sellest, kuidas organisatsiooni riskijuhtimine on korraldatud ja strateegiliste eesmärkidega seostatud. Meetodi uudsus peitub selles, et see võimaldab kasutada analüüsiks juba kogutud informatsiooni, kuid toob otsustusprotsessi rohkem selgust justnimelt läbi riskide eristamise. Kasutatakse küll sama informatsiooni, mis juba on infoturbe spetsialistide käsutuses, kuid tuues paremini esile need tuvastatud riskifaktorid, millel on suurem mõju terve organisatsiooni kontekstis.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 54 leheküljel, 6 peatükki, 19 joonist, 24 tabelit.

Acknowledgements

I would like to express my deepest gratitude to Professor Hayretdin Bahşi for his patient guidance, encouragement and enormous support. Many thanks to Patrick for the help and valuable suggestions. Thank you Liisu for standing by my side and translating into Estonian.

Finally, I would like to thank my family for their continuous support and unparalleled love.

Without you, I would not have been able to do it.
Thank you all!

List of abbreviations and terms

AIS	Accounting Information Systems
AHP	Analytic Hierarchy Process
ANP	Analytic Network Process
CEO	Chief Executive Officer
CIA	Confidentiality, Integrity, Availability
CISO	Chief Information Security Officer
COBIT	Control Objectives for Information and Related Technology
CR	Consistency Ratio
DPO	Data Protection Officer
FCA	Financial Conduct Authority
GDPR	General Data Protection Regulation
Fintech	Financial technology
HCST	High Cost Short Term
HR	Human Resources
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
ISACA	Information Systems Audit and Control Association
ISC^2	The International Information System Security Certification Consortium
ISM	Information Security Manager
ISMS	Information Security Management Systems
ISO	International Organization for Standardization
ISRM	Information Security Risk Management
ITIL	Information Technology Infrastructure Library
MCDM	Multiple Criteria Decision Making
PII	Personally Identifiable Information
SD	Super Decisions Software
SYMBIOSIS	Security Metrics and Business Objectives

Table of Contents

List of Figures

List of Tables

1. Introduction

This chapter provides an introduction of the topic explaining motivation for the thesis, raises the research problems needed to be treated. Also it reveals goals and objectives to achieve along with scope and assumptions. In the end, it elaborates on what this thesis will contribute further.

1.1 Motivation

In an environment where information technology is present in every bit of it, the importance and challenges of dealing with its risks increase significantly. Therefore, for an information security professional it becomes vital to get organized dealing with such problems in a way that one's roadmap converges with what organizations objectives are. Information security teams have a hard task to keep the right balance between maintaining assets, systems and networks secure and compliant, while being assured that information security team is satisfying supporting business objectives. Classifying risks into some levels does not tell clearly the importance between information assets as this categorization is business oriented. For this reason prioritization of risks needs to be aligned also with organization's goals. While working in the industry as an information security analyst, I have seen this as a problem worth tackling and necessary to be addressed.

The need to have IT risks aligned with overall organization's strategic objectives becomes even more important when the number of these risks and stakeholders increases. Since this concerns everyone, it would be very beneficial to find a way which would help in focusing on the most crucial risks, while at the same time having assurance that dealing with them has brought the impact at the right place. By having risks prioritized and in synchronization with overall strategic objectives of the organization, it is more convenient for information security teams to know where their focus will and should be.

The benefits of alignment would be mutual: business decision makers would be ensured that IT security supports their objectives and might be encouraged to provide more financial support and information security team on the other side knows that it is providing value, not only from technical but also business operation perspective without having to change their scope. If information technology risks are not properly aligned with key objectives,

the probability of them impacting overall institution increases dramatically. I believe that by such alignment, the information security team will be able to have a better focus and collaborate better with stakeholders about these risks, with aim to ensure that they are supporting the organization in achieving the objectives.

Studies emphasize that although it depends on organization, usually strategic goals are expected to remain the same for some years [29] [58]. Hence, because this stability knowing and adjusting focus of information technology risk management that support these goals, will be beneficial. If strategic goals are not taken into account from risks, shifting to them later it might turn out to be costly and in a worse scenario not possible at all due to time, lack of resources, and/or preparations.
Multiple Criteria Decision Making methods (MCDM) are used when several alternatives are to be considered and prioritized among each other, based on defined criteria. They direct the decision maker towards best alternative(s), based on the judgments that he/she has made to these criteria and alternatives, by comparing them among each other. Such methods have found large applicability in fields of strategic decision making [28] [18],[15], evaluation performance [44], supplier selection [27], [79] etc. In this study strategic goals are our criteria and information technology risks are the alternatives.

1.2 Research problem

The research questions that I raise in this study are:

- How can information technology risks be prioritized based on strategic planning goals?
- Will strategic goals have any impact on risk ranking using methodology proposed?
  - If there will be impact over risk ranking, how much they will be differentiated between each other?

By using AHP and ANP as two MCDM methods, integrated together for risk alignment with strategic goals, we should be able to rank these risks. This ranked list should serve as a guide for information security team to ensure support for the organization towards reaching its objectives and at the same time manage information security risks.

1.3 Goal, scope and assumptions

This thesis, aims to provide a mean of aligning strategic goals with information technology risks based on existing multiple-criteria decision-making methodologies (AHP and ANP)

for prioritization. In scope of this study there will be strategic goals of the organization, set by decision makers and information technology risks identified by information security team. It is important to state that this thesis does not focus neither in determining how strategic plan is made, nor identifying information security risks process. Instead, they are accepted as they are and other studies would better determine their efficiency and appropriateness.

In order to apply the proposed methodology for effective alignment of risk management with strategic goals, a number of criteria need to be meet:

- The organization needs to have clear strategic goals
- Organization has clearly identified information security risks.
- The organization has a qualified person/team in charge of dealing with information security or experience on information security.
- The collaboration between different teams is well organized and organization has a good flow of information.

For the study, it will be assumed that time is not a factor that needs to be considered for prioritization, as urgency for dealing with a certain risk would add another dimension to consider. The method that I am going to propose, should be flexible enough to allow new strategic goals and/or risks to be part of it, even after it has initially been conducted. It would be up to information security team when to integrate new risks or make changes to existing ranking cycle.

1.4 Novelty

The novelty of this master thesis lies on bringing together strategic goals and risk management and produce risks ranked as output. This output, not only should direct information security team to build a roadmap and guide them on what to work on for the next periods of time, but also will help them to be synchronised with major goals of the organisation. This is important considering that prioritizing risks is not an easy task, as many factors have to be taken into account (priorities, resources etc).

Having clear objectives helps to concentrate resources and when risk management is on the same direction with strategic objectives they would produce more value [22]. The existing studies do not engage with this issue specifically and therefore I believe it will bring a good perspective to look into. The way that decision making methodologies adopted in this thesis deal with the problem is new. The integrated AHP and ANP, fits best for the type of problem I am dealing with and they are widely used in many fields that require

ranking in decision making (refer to section 2.1.2). In addition, in Chapter 4 I bring also a use case organization, where I apply the proposed methodology.

2. Background information and Literature review

This chapter gives background information about strategic goals,risk management and how they are important to be synchronized for the organization. Then, it explains study and introduces the reader with methodologies that are used in the thesis, why they are chosen and gives a description of standards that serve as guidance for information security risk management and alignment with strategic goals as an major part of business success. Further, it discusses about studies that are already conducted for the topic and their identified gaps.

2.1 Background information

2.1.1 Strategic goals and information security risks

The use of information technology comes at a price since there is some skepticism on investments in IT and strategic planning. As Tallon and Kraemer have found, this uncertainty comes due a curve in return on investment: *"There is an increase benefit from IT but up to certain point, after which more investments do not return the same level of benefits. This goes in hand also for IT risk management as an important part, not only IT but the business itself"* [71]. To back up that, Jenkins and Williamson claim that it is essential that everyone needs to know targets derived from strategic objectives continually, in order to know and add them to their daily operations and hence they will have a clear picture of where they should focus [39]. Significant role on this regard is played from frameworks which provide best practices of using information technology in business operations. ITIL takes a general approach toward the impact that information technology should play organizations and guides on harmonizing it with business strategy [6], ISO31000 provides guideline for risk management as part of IT management [38] and COBIT is a framework for risk management that encourages involvement of stakeholders for an effective risk management, fill in gaps in technology operations, practices and procedures, active risk communication throughout the organization and resource allocation in order to help information security experts to tackle the risk management issues [21].

Chandler defines strategic goals as the determination of the basic long-term objectives for an organization by adopting the course action and the allocation of resources for carrying out these goals [11]. Rapid7 defines information security risk management as:
"The process of managing risks associated with the use of information technology and it involves identifying, assessing, and treating risks to the confidentiality, integrity, and availability of an organization's assets" [57].

Thus, an effective information security risk management supports the organization by assisting to reach strategic goals by protecting the organization's assets, systems, operations, customers data, reputation etc. Calculating the value of an information technology is a difficult task [45] and my research does not intend to suggest a way to quantify that in a number but it does require it to be considered in analysis from the stakeholders, in terms of its impact in each domain[1] with respect to higher organization's strategic goals set by decision makers.

Following sections give an insight of each of the methods, their principles and standards used in this thesis.

2.1.2 Choosing Multiple Criteria Decision Making method

The methodologies used on decision making when multiple alternatives are to be considered as solution(s) are called Multiple Criteria Decision Making methodologies (MCDM). These methodologies require that the decision maker identifies the criteria that he/she is interested and alternatives that are connected to it. These relationships of criteria and alternatives are done by setting weighting values, thresholds or preferences based on the type of the problem. There is no best MCDM method, because that depends on the nature of the problem but are various studies discuss on how to choose the right MCDM method [46], [72]. According to Baker et al. citing Mota, Campos, and Neves-Silva, when choosing MCDM it is necessary to consider aspects such as: type of the problem and its scale, number of alternatives, ability to consider new alternatives, incompatibility and conflict, organization of the alternatives, nature of the alternatives set, data type, measure scale, criteria weighting and interaction,tools available, end evaluations etc. Using the tool created by Munier [47] and considering the nature of the topic:many criteria, independent alternatives and criteria, nature of alternatives, necessity to evaluate relative importance, tools available and familiarity with using these tools, AHP and ANP were chosen. I addition as described by Saaty AHP (and therefore also ANP) can be approached with absolute values [60] [48] although this might reduce the quality of data. Other

[1] *The subject area to which the user applies a sphere of knowledge, influence, or activity ...* [68]

methodologies to consider were TOPSIS (does not allow independent alternatives and criteria, an alternative cannot be part of different scenarios), PROMETHEE and ELECTRE (they do not allow independent alternatives and criteria) [47]. Furthermore AHP and ANP are used in numerous fields, either separate, together or combined with other methodologies, depending on characteristics of the problem needed to be solved.

Analytic Hierarchy Process

Analytic Hierarchy Process is a theory of measurement developed by Thomas L. Saaty in early 1970s and improved throughout years [26], that uses experts reasoning by pairwise comparisons between elements of the same group (criteria or alternative) using Saaty's scale (section 2.1.3) [59]. AHP is a top-down method which means that criteria influences alternatives but not vice versa.
AHP is based on three principles:

- Decomposition - a structure is required to capture the elements of the problem as shown in Figure 1. This means that criteria and alternatives need to be identified clearly for the problem.
- Comparative judgement - pairwise comparisons are done for each alternative with respect to the criteria in a higher level. Ranking of criteria is calculated based on what is considered as control criteria (Figure 1 shown as Goal on top of the hierarchy). Pairwise for Criteria Goal is done between Criterion 1, 2 and 3 as alternatives. Pairwise for Criterion 1 is done between Alternative 1 and 2 and the same is done for Criterion 2.
- Synthesis of priorities - priorities are synthesized starting from the second level (Criterion 1, 2 and 3) and down (Alternative 1 and 2) multiplying priorities of that level and the level below that as shown in Figure 1.

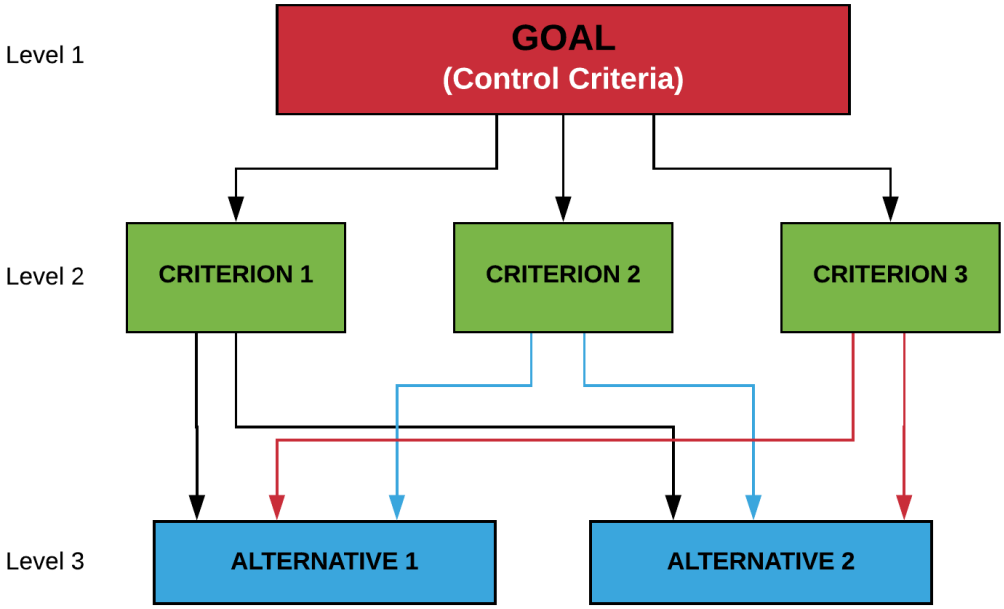

Figure 1. General model of AHP
[61]

In Figure 1, criteria 1, 2 and 3 are pairwise compared with each other with respect to control criteria to determine which one is the most important for the Goal (control criteria).

AHP operates under four axioms [67]:

- *Reciprocal pairwise comparison between two elements is equal to 1.* [2].
- *Each level of hierarchy is not depended from the lower level in the hierarchy.*[3].
- *Homogeneity- two elements are comparable against each other.*
- *The problem needs to be known very well when using AHP, so to have every aspect taken into account.* [4]

Analytic Network Process

Analytic Network Process derives from AHP as a general form of it and is based on the principles and axioms of AHP but a network relationship is applied instead of a hierarchy: not only criteria influences on alternatives but also alternative's importance play their role on criterion. So, not only Criterion 1 importance is evaluated on Alternatives 1 and 2 but

[2] *If alternative 1, is two times more preferred than Alternative 2, then Alternative two is two times less preferred than Alternative 1 (2 for Alternative 1 and 1/2 for Alternative 2)*
[3] *Dependency known also as correlation in statistics, shows relationship between two variables*[30]
[4] *In connection with decomposition principle*

also the importance that these two alternatives have on Criterion 1.

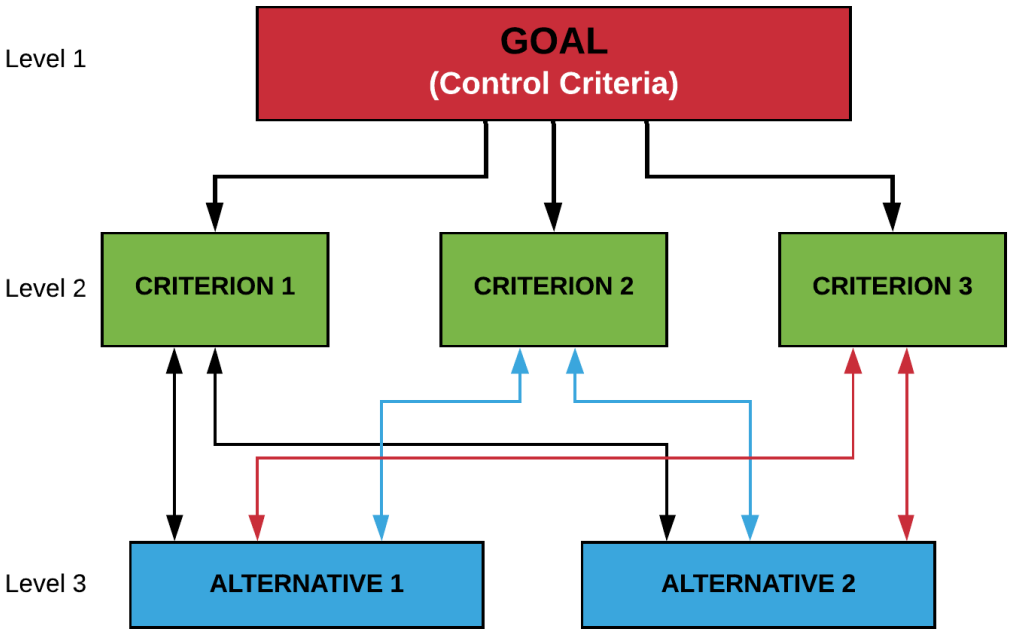

Figure 2. General model of ANP
[63]

Characteristics of ANP described from Saaty in "Fundamentals of the analytic network process" are [63]:

- ANP is a general form of AHP since also alternatives have importance for criteria.
- By allowing for dependence, the ANP it allows also independence making it a special case of AHP. User can choose to not apply importance of an alternative towards criteria.
- Dependence in ANP can be not only within elements of the same cluster, but also outside of it. [5].
- Since there is no hierarchy in ANP, there is no strict rule of which problem gets analysed first.
- ANP can provide ranking not only for alternatives but also clusters.
- By relying on control elements, ANP can provide a mean to deal with different criteria, which comes handy if user interested to include costs, benefits, opportunities and risks for his/her problem. [6]

[5]Clusters in AHP/ANP are elements grouped together (criteria, alternatives)
[6]In relation with point three of characteristics of ANP.

Following is a hypothetical example for buying a security product (firewall, vpn, antivirus). In this example security features and technical support are criteria and Product A and Product B are alternatives. If weights for criteria are: security features (0.6) and technical support (0.4) and on each Product A scores (0.33, 0.8), while Product B scores (0.66, 0.2). Also, we assume that Product A has relatively good security features and good technical support (0.5 and 0.5 with respect to each criterion), while Product B has very good security features but poor technical support (0.8 and 0.2 with respect to each criterion).

If we use AHP, then Product A with 52% will be chosen to 48% for Product B [7]. But if we use ANP, then we would choose Product B with 50.3%, because its very excellent security features that it has, will also play a role in decision, something that was not taken into consideration in AHP (refer to 2nd Axiom in AHP section 2.1.2). [8] The example is illustrated in Table 1.

Table 1. Example of using AHP or ANP for buying a security product

		AHP Applied			
		Security Features	**Tech support**	**Product A**	**Product B**
Security Features	0.6			–	–
Technical support	0.4			–	–
Product A	52.0%	0.33	0.8		
Product B	48.0%	0.67	0.2		
		ANP Applied			
		Security Features	**Tech support**	**Product A**	**Product B**
Security Features	0.6			0.5	0.8
Technical support	0.4			0.5	0.2
Product A	49.7%	0.33	0.8		
Product B	50.3%	0.67	0.2		

AHP has found application in manufacturing [8], transport [54], security policy decision making [33], environment impact assessment [55], military [13] [14] and in IT field: prioritization [43], network selection [12], software selection [24], resource allocation [16],[56], project delivery [2], healthcare risk factor assessments [51].

ANP has been used in location selection [17], IT product and vendor selection [52], [9], [20], e-shopping [3], supply chain risk evaluation [78], information security risk control assessment [80], use of ICT in enterprises [10].

Both **AHP and ANP** are used for decision making and prioritization in problems where there are dependencies and inter-dependencies in fields of economics[65], public binding

[7] 0.6*0.33+0.4*0.8=51.98 vs 0.6*66+0.4*0.2=0.4802

[8] *Because ANP calculations are complex SuperDecisions software was used.*

Table 2. Saaty Scale [62]

Intensity of Relative Importance	**Definition**	**Explanation**
1	Equal importance	Two activities contribute equally to the objective
3	Moderate importance of one over another	Experience and judgment slightly favor one activity over another
5	Essential or strong importance	Experience and judgment strongly favor one activity over another
7	Demonstrated importance	Experience and judgment strongly favored and its dominance is demonstrated in practice
9	Extreme importance	The evidence favoring one activity over another is the highest possible order of affirmation
2,4,6,8	Intermediate values between the two adjacent judgments	
Reciprocals of above non-zero numbers	If an activity has one of the above numbers assigned to it when compared with a second activity, then the second activity has the reciprocal value when compared to the first (From Axiom 1)	

[50], public project prioritization [42], project investment [5], determining priorities for maintenance strategies [82] and interdisciplinary (economics, sports and social life) [1] [64] [83].

2.1.3 Saaty scale and Consistency Ratio

Two very important elements that we need to know when using AHP and ANP are Saaty's scale and CR.

Saaty Scale

Saaty Scale is used for pairwise comparison between two elements with respect to a node.[9] Table 2 shows the ratio scales for pairwise comparison in AHP and ANP.

Ishizaka's proposes a method with clusters and pivots for alternatives preordered by making the problem as single criterion. This method consists on doing pairwise comparison of alternatives for one criteria and based on that, do all other comparisons and helps when a large number of comparisons needs to be done[34]. Ishizaka's approach is shown in Table

[9] *A node is another element which can be either a criterion or another alternative*

Table 3. Cluster of 5 [Ishizaka A.] [34]

Level	L9	L8	L7	L6	**L5**	L4	L3	L2	L1*
L9	1	2	3	4	5				
L8		1	2	3	4				
L7			1	2	3				
L6				1	2				
L5					①	2	3	4	5
L4						1	2	3	4
L3							1	2	3
L2								1	2
L1									1

3.

An extended version of Ishizaka's approach in Table 3 would be Table 4 although this would require more pairwise comparisons. In our case the same level scale as Saaty is used, but with only change of measuring alternative's absolute importance for criterion with level 1 (minor or no importance) to level 9 (extreme importance.) The matrix explains levels of pairwise comparisons with each other. For instance: when comparing Level 7 (Demonstrated importance) in Y axis as base, with Level 1 (Minor or no importance) in X axis as secondary element, it means that Y axis element is 7 times more important than X axis element. The diagonal of cells left to right shows that for the same levels, the importance is the same. For example, if elements A and B are essential for the criteria (level 5), they are of the same importance compared to each other. The remaining of cells are the reciprocal values. For base element as 1 and second element as 7, this value is 1/7 (Y=1 and X=7 value is $\frac{1}{7}$) or 7 times less important (Axiom 1 in AHP section 2.1.2). This comparison is consistent also in software used for use case and gives low levels of inconsistency values [10] consistent with Ishizaka model. These values range between 0.013 to 0.035, way below threshold 0.1.

Table 4. Extended version of Ishizaka [34]

Level	L9	L8	L7	L6	**L5**	L4	L3	L2	L1*
L9	1	2	3	4	5	6	7	8	9
L8		1	2	3	4	5	6	7	8
L7*			1	2	3	4	5	6	7*
L6				1	2	3	4	5	6
L5					①	2	3	4	5
L4						1	2	3	4
L3							1	2	3
L2								1	2
L1			1/7*						1

[10] Inconsistency values are explained in following section.

Consistency Ratio

Citing Kent and Williams, Saaty defines consistency ratio (CR) as ratio of consistency index for a set of judgements, with that of random comparisons for a matrix that has the same size [41]. CR derives from mathematical principle of transitive relation: if A is preferable to B and B is preferable to C, then A is preferable to C [25]. This indicator is calculated from dividing CI (Consistency Index) with RI (Random index), where CI is deviation of consistency for the set and RI is the consistency index of randomly generated pairwise matrix with values known, for n items compared (items can be criteria or alternatives, depended on what we are comparing) (Table 5)[59] [77]. As it can be seen in Table 5 inconsistencies start when the number of alternatives that need to be considered is more than two (as no inconsistencies are expected for only two alternatives).

$$CR = \frac{CI}{CR}$$

Table 5. Random Consistency Index - RI - (for n items compared)

[77]

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
RI	0	0	0.58	0.9	1.12	1.24	1.32	1.41	1.45	1.51	1.51	1.48	1.56	1.57	1.59

AHP and ANP do not have validation methods but as Saaty suggests in several researches, the value of CR should be up to 0.1 in order to have reliable results. [59] [63] [66] [11]

2.1.4 Contextualization

The study in this thesis needs to get context of relationships between elements. Various approaches are available but usually they are focused specifically in one particular field or purpose: Business (COMPRO [23], Business Process Domain Views[49]), Information technology (Domain Based Security- SCADA [40], ConTaaS: Internet-Scale Contextualisation [81]) Human Sciences (Progressive contextualization-used in ecology science [73], etc.)

SYMBIOSIS (SecuritY Metrics and BusIness ObjectiveS, Integrated and Synchronised) is a methodology that does mapping of business processes to security goals by using templates for contextualisation [53]. This methodology eases the process of identifying a goal and helps toward mapping alternatives for that goal, by capturing these predefined

[11] Please note that CR in SD software used in this research is represented by inconsistency rate instead, and is equal to 1-CR.

elements. Using SYMBIOSIS, we can be assured that: metrics of criterion are going to be captured in a top-down way while being on their granular mode and impact of these metrics can be followed also from bottom up [53]. This methodology was chosen as most appropriate for mapping strategic goals, domains and risks.

SYMBIOSIS suggests information collection in four steps:

1. Define main business objectives
2. Define how security goals will be measured
3. Derive security metrics using security measurement questions and stakeholders of security goals
4. Utilise security metrics by conducting security measures, provide feedback and reflect the findings into business objectives

The template proposed from SYMBIOSIS as shown in the Table 6, requires elements identifying multiple aspects of the goal, so nothing will be left out in analysis with respect to its components that this particular goal is related to.

Table 6. Formalised Business Objective [53]

Identifier	Unique identifier for the business objective.
Object	The system/domain the objective focuses on.
Scope	The system/domain that affect or are affected by the objective.
Purpose	What is the aim with regard to the object within defined scope.
Viewpoint	Who are the stakeholders are of the objective.
Context	Aspects to consider towards purpose achievement (costs, laws and regulations and other resources needed)
Relationship to other objectives	What other business objectives may affect or be affected by the objective

2.1.5 ISMS and ISO27000 Standard Family

ISO defines an ISMS as:
"Policies, procedures, guidelines, and associated resources and activities, collectively managed by an organization, in the pursuit of protecting its information assets. An ISMS is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's information security to achieve business objectives." [36]

In order for a company to ensure that is properly dealing with all security aspects of its operations, a set of documentation is required to be in place and cover all operations.

ISO standards are internationally best practices tailored and accepted by experts which set minimal basic requirements for operations. These standards serve as a guideline to ensure that organizations that follow them have handled all aspects that would concern the organization on operations, products and services.

ISO27000 family is a set of affiliated standards that address specifically information technology security. ISO27000 standard provides a general description of the rest of standards and sets the grounds on vocabulary [36]. The rest are identified as standards that concern: requirements (27001, 27006 and 27009), guidelines (27002, 27003, 27004, 27005, 27007, 27008, 27013, 27014, 27016, 27021) and specific sectors, inter-sectors and inter-organizational communications (27010), telecommunications organizations (27011), cloud services(27017), PII (27018) and energy utility industry (27019). ISO 2703x and 2704x are designed for control-specific guidelines [36].

The ISO27001 standard is of particular interest for our study since it lays the foundations for other ISO2700 standards by dividing all organization's operational aspects into 14 domains [37]. Sanchez and Vilariño define a domain as: *"The subject area to which the user applies his/her activity, knowledge, influence etc. ..."* as part of the operations. [68].

The 14 domains and their corresponding objectives described in ISO27001 [37] are:

- **A.5 Information security policies** - provides guidance for information security regarding business requirements, laws and regulations.
- **A.6 Organisation of information security** - aims to help information security to set up a solid framework for information security.
- **A.7 Human resource security** - guides for best practices regarding information security for employees and contractors, before, during and after the agreement with them).
- **A.8 Asset management** - helps to ensure that all assets will receive necessary security protection and support CIA.
- **A.9 Access control** - helps to ensure safeguarding and control access towards systems and assets.
- **A.10 Cryptography** - guides to best practices of using cryptography for CIA.
- **A.11 Physical and environmental security** - guides for restricting unauthorized physical access to systems, assets and operations.
- **A.12 Operations security** - guides towards security operations with respect to information: prevent loss of data, ensure CIA, limit vulnerability exploitation and event logging.
- **A.13 Communications security** - ensure protection of networks, systems and data

transfer in and out of organization.

- **A.14 System acquisition, development and maintenance** - helps to make information security part of every process in development life cycle and reliable testing.
- **A.15 Supplier relationships** - directs towards best practices of ensuring CIA of organization's assets that are accessible from third parties.
- **A.16 Information security incident management** - guides to all aspects in response to security incidents.
- **A.17 Information security aspects of business continuity management** - provides best practices concerning availability of operations for the organization.
- **A.18 Compliance** - guides how information security should help the organisation to approach legal and regulations aspects towards customers, employees and third parties.

2.1.6 COBIT

From ISACA, COBIT is described as a framework that aims to guide the entire organisation in terms of governance and management of information technology with primary objective to achieve goals in its entire structure and covers information security risk management. Referencing particularly "Governance and Management Objectives" set by COBIT, concern: goal aligning of IT related objectives with enterprise strategies and meeting expectations of decision makers for IT (EDM01), stakeholder engagement for roadmapping, IT objectives and roadmapping (EDM05) and other objectives go hand in hand with ISO27001 domains (HR-AP07 optimise human resources for reaching goals, suppliers and risk management for reaching organization's major objectives -AP08/AP10). [21]

2.2 Related work

The problem of aligning strategic goals and information risk management is not new, as researches have been done in studying relationship of information technology and organization's strategies: [73], [31], [53]. The role of the information security risk management in reaching goals for organization has been focal point of studies for Schermann et al. [69], Wilkin and Chenhall [76] and IBM [32].

Schermann et al. take a broad overview of IT risks, recognize the importance of understanding risks well when it comes to risks role in goal success rate but it focuses only in risk project level, which means that it has a narrow scope. Therefore, this study shows the benefits of a proper risk management suitable in project level but does not provide a

method can be used for high strategic goals of the organization as an entire unit. [69]

Wilkin and Chenhall conduct a literature review for IT risk management, strategic alignment and resource management to identify future research and areas in relation to each other. In addition to that, their focus for these fields is oriented solely in Accounting Information Systems. [76]

A white paper from IBM, does identify important problems such as: executives scepticism in IT for risk management, limitations of finding the risk metrics for IT risk measure and the benefits of having strategic goals and IT risks aligned together. The approach on this study is that of separating the whole scope of the organization in only six domains (People, Processes, Technology, Suppliers, Infrastructure and Exostructure[12]). For a big organization, merging all domains together will make it hard to evaluate the role of domains in strategic goals. In addition, domains proposed from IBM do not mention very important aspects such as business continuity and compliance. The paper also sees these domains only from the perspective of business operations and not from the information technology perspective. Hence, a holistic perspective which would include both information technology and business goals is essential but missing in this paper [32].

Where all these studies and researches pinpoint, is the need to have a well established IT risk management approach which not only takes into consideration strategic goals set from decision makers but also put that into practice in a simplified model such as a roadmap type, easy to be understood and usable from anyone. These studies and the large applicability of decision making methodologies that I have chosen are proven in other fields, make the foundations of a solid approach on what I am recommending, towards providing a mean of filling in these gaps.

Consequently, this proposition brings a substantial assurance that it will be beneficial for those who deal information technology risks. Information security team will have in scope all domain prone to information security risks and be in the same direction with the decision makers. This will provide an understandable way of how information security helps to reach, not only its goals but also support to reach major objectives of the organization.

[12] *Critical components usually outside of the organization's control.*

3. Research methodology

This chapter introduces the reader with research design, how the methods work on the problem and validity of methods used. Also, it informs on how the use case process is conducted and software used for the use case. The methodology is a combination of qualitative and quantitative approach. The input needed is qualitative as perception and judgement is required and the output is quantitative as it provides a ranking based mathematical model applied.

3.1 Research Design

This section describes how information security risks and strategic goals, come together using ISO27001 domains as an intermediate component and provide ranked list of risks, aligned with strategic goals.

Figure 3 shows the research design and the flow process of the study in steps. AHP is applied from step 1 to step 6 and from step 7 to 13 ANP is applied (using as input the output of ANP) as explained onward.
The study starts with **step 1**, with a list of strategic goals set from decision makers of the organization. In **step 2**, decision maker uses SYMBIOSIS based template (Table 11) with Saaty based Scale Table 2 to do mapping of domains over goals. In this step, help of CISO/ISM is required since decision maker might not be familiar with what is covered on each domain of ISO27001 (refer section 2.1.5). In **Step 3**, we will have information about goals captured and we are ready to do comparison using Table 4. Information for step 2 and 3, can be collected with tools such as Google Sheets, Microsoft Excel, LibreOffice Calc or similar. In **step 4**, by entering information collected in step 3, goals are compared as criteria and domains are compared as alternatives of AHP using Table 4. In **step 5**, goals are pairwised to overall organizations objectives and domains are pairwised respect to the goals identified in Step 1. This information is used from SD in **step 6**, to do ranking of goals (6B) with respect to organization (6A) and ranking of domains (6C) with respect to overall goals (6B) identified in step 1. This step is the last one concerning organization's goals and domains ranked based on them. Goal ranking (6B) and Domain ranking (6C) are used as control criteria later in step 12 (as 12A).

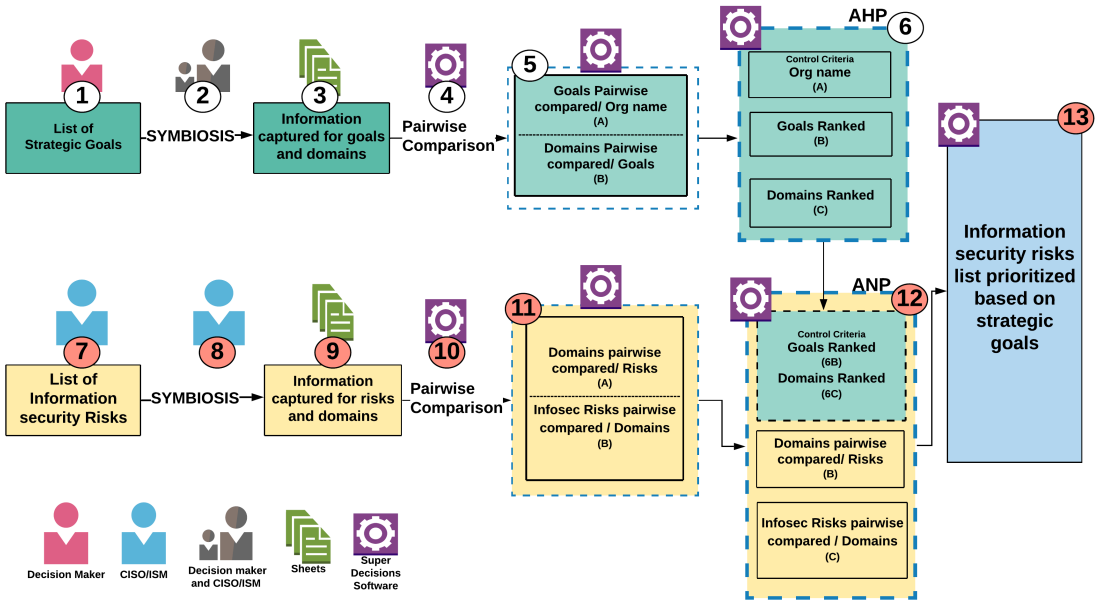

Figure 3. Cahani model

In Figure 3, from step 7 onward, the ANP process is initiated. In **step 7**, a list of information technology risks identified is needed for the cycle. Steps 7 to 13 need to be done for every risk category that organization has (for example low, medium, high). In **step 8**, CISO/ISM uses again SYMBIOSIS based template (Table 11) and Saaty Scale (Table 2) to identify relationships and do mapping between risks identified in step 7 and domains from ISO27001 (section 2.1.5). In **step 9**, we will have information about risks and domains captured and we are ready to do pairwise comparison using Table 4 in the next step. Information in steps 8 and 9, can be collected with the same tools as in steps 2 and 3. In **step 10**, SD is used to do pairwise comparison between risks for each domain and comparison between each domain, as explained in ANP section 2.1.2. In **step 11**, information on pairwise domain comparison based on risks (11A) and risks pairwise comparison based on domains (11B) is calculated in SD and ANP can be applied. In **step 12**, ANP is applied with Goals Ranked (6B) as control criteria, Domains Ranked 6C [1] and domains pairwise compared in 11A as criteria and pairwise compared information security risks (12C) as alternatives [2] (refer to ANP structure in section 2.1.2). Finally in **step 13**, ANP is applied over control criteria, criteria and alternatives and SD gives a prioritized list of information security risks based on strategic goals. [3]

Prioritized list of risks that results from this methodology, reflects the impact of strategic

[1] Notice that Goals Ranked (6B) and Domains Ranked (6C) together make 12A, when applying ANP.

[2] Domains pairwise compared/ Risks (12B) and Infosec Risks pairwise compared/ Domains (12C) are the same as Domains pairwise compared/ Risks from (11A) and Infosec Risks pairwise compared/ Domains (11B)

[3] Steps 1-5 and 7-11 although they treat different subjects, are in executed in the same way.

goals on one side and information technology aspects (risk levels assigned in the beginning) from the other. This list then, serves as a guideline and enables information security team to focus on providing more value for the organization from the security of information technology perspective.

3.2 Measurements and use case sample

Using the methods mentioned in research design, CEO and ISM of organization were required to provide their perception of importance for every element taken into the study. First, the CEO of company was required to evaluate the importance that every goal has for the company to determine ranking of goals. Then, with the help of ISM (to provide expertise in domains), for each of these goals the importance of the goal was evaluated on each domain using Saaty's based scale (1-minimal importance to 9 extremely important).

The risk evaluation method that organization uses is the model:

$$\textbf{RISK} = \textbf{LIKELIHOOD} \times \textbf{IMPACT}$$

These risks are calculated as a product of threat likelihood with magnitude of its impact as described from Steinberg guideliness [70] shown in the Table 7 and Table 8.

Table 7. Threat likelihood [70]

Likelihood	**Definition**
High	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective
Medium	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

Table 8. Magnitude of impact [70]

Impact	Definition
High	The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Medium	The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
Low	The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

Organization uses a risk assessment with levels of risks labeled as low, medium and high. Roles that are required to conduct the study are: the decision maker(s) that determines strategic goals and the ISM who maps every domain for risks and assists decision maker the same process on goals. Intermediary role profiles such as a Chief Technology Officer or a IT business analyst, could be useful in explaining relationships between business and information technology aspects. The roles and the part played in the study are illustrated in Figure 3.

3.3 Data Collection Process

A list of strategic goals was required from decision makers of organization (step 1 in Figure 3), along with a list of risks and their importance provided from ISM to initiate the study (step 7 in Figure 3).

In order to determine importance for goals with respect to the organization (to find out which are the most important goals for organization) and to capture information about importance that risks have for the domain (steps 2 and 8), template Table 9 is used.

Table 9. Template for information capturing for information for control criteria and domains

ID Organization/Domain Name	Level of importance
Name of goal/risk	Level of Importance
....	Level of Importance
Name of goal or risk	Level of Importance

For organization, the ID consists of the name of the organization while scope includes

Table 11. Template for information capturing

ID Name of Goal or Risk	**Level of importance**
A.5 Information security policies	Level of Importance
A.6 Organisation of information security	Level of Importance
A.7 Human resource security	Level of Importance
A.8 Asset management	Level of Importance
A.9 Access control	Level of Importance
A.10 Cryptography	Level of Importance
A.11 Physical and environmental security	Level of Importance
A.12 Operations security	Level of Importance
A.13 Communications security	Level of Importance
A.14 System acquisition, Dev. and maintenance	Level of Importance
A.15 Supplier relationships	Level of Importance
A.16 Information security incident management	Level of Importance
A.17 InfoSec aspects of BCM	Level of Importance
A.18 Compliance	Level of Importance

names of goals and their importance with respect to the organization. Level of importance for domain over goal/risk.

The list of goals provided from use case organization (step 1) and the importance given for each of them, is shown in Table 14 (step 2 in Figure 3.) Goals are compared to control criteria "Use case Organization", towards determining the ranking of each goal for the organization (step 2 in figure 3).

Table 10. Goal's Importance for organization

ID- Use Case Organization	**Level of importance**
Goal 1	7-Very high
Goal 2	8-Important
Goal 3	6-High
Goal 4	4-Low medium
Goal 5	5-Medium
Goal 6	5-Medium

At the same time for step 2, using the SYMBIOSIS template (Table 11), information about domain importance for goals is captured using Saaty's based scale (Table 2).

Information for "Goal 1" is given in Table 12. The information captured for other goals can be found in section A.4.1 in Appendix.

In step 4, when pairwise comparison is done between goals, the relative importance is calculated with respect to organization. Also in the same step, pairwise comparison between domains is done with respect to each goal.

Table 12. Information capturing for Goal 1

ID Goal 1	**Level of importance**
A.5 Information security policies	5-Medium
A.6 Organisation of information security	1-Minor/No importance
A.7 Human resource security	4-Low Medium
A.8 Asset management	1-Minor/No importance
A.9 Access control	4-Low Medium
A.10 Cryptography	3-Low
A.11 Physical and environmental security	1-Minor/No importance
A.12 Operations security	6-High
A.13 Communications security	3-Low
A.14 System acquisition, Dev and maintenance	8-Important
A.15 Supplier relationships	9-Very important
A.16 Information security incident management	8-Important
A.17 InfoSec aspects of BCM	9-Very important
A.18 Compliance	8-Important

Table 13. Direct comparison between goals with respect to organization

	Goal 1	**Goal 2**	**Goal 3**	**Goal 4**	**Goal 5**	**Goal 6**
Goal 1	1	1/2	2	4	3	3
Goal 2		1	3	5	4	4
Goal 3			1	3	2	2
Goal 4				1	1/2	1/2
Goal 5					1	1
Goal 6						1

Using Table 4 to compare organization's goals based on information collected for goals importance for organization (Table 10), it can be determined that Goal 2 is twice more important than Goal 1 (first cell of second row, first column) in Table 13. In the same way Goal 1 is twice more important than Goal 3 (compare Goal 1-Very high importance with Goal 3-High importance), four times more important than Goal 4 (compare Goal 1-Very high with Goal 4-Low medium importance).

In the same way for Goal 1 in Table 12, domain A.5 Information security policies is five times more important than A.6 Organisation of information security. With goals pairwise compared (step 5A Table 13) and domains pairwise compared (step 5B), we were ready to proceed with final results of AHP in step 6. Results are shown and discussed in Chapter 4 and are used in step 12.

The list of information security risks (step 7 in Figure 3) provided is as shown in Table 14.

First, risks are separated in groups, based on their risk level as low, medium and high, and for each of them steps 7 to 13 are done separately. For each risk, the importance of domains

Table 14. Risk Level List for Organization

Risk Observation	**Risk Rating**
Risk 1	High
Risk 6	Medium
Risk 8	Medium
Risk 10	Low
Risk 13	High
Risk 14	Low
Risk 16	Medium
Risk 17	Medium
Risk 18	Medium
Risk 20	Low
Risk 22	Medium
Risk 23	High

Table 15. SYMBIOSIS for Risk 1

ID	**Risk 1**
A.5 Information security policies	5-Medium
A.6 Organisation of information security	1-Minor/No importance
A.7 Human resource security	1-Minor/No importance
A.8 Asset management	1-Minor/No importance
A.9 Access control	1-Minor/No importance
A.10 Cryptography	6-High
A.11 Physical and environmental security	1-Minor/No importance
A.12 Operations security	7-Very high
A.13 Communications security	8-Important
A.14 System acquisition, Dev and maintenance	1-Minor/No importance
A.15 Supplier relationships	1-Minor/No importance
A.16 Information security incident management	7-Very high
A.17 InfoSec aspects of BCM	1-Minor/No importance
A.18 Compliance	5-Medium

is captured using SYMBIOSIS template based (Table 11) as defined from step 8 in Figure 3. For each domain, the importance of risks is recorded using the other SYMBIOSIS based template (Table 9) as defined from step 8 to collect information for risks.

Table 15, shows information collected for Risk 1 and Table 16 shows information collected for domain A.5 as example (step 9 in Figure 3). The rest of this information can be found in Appendix section A.4.3.

Table 16. SYMBIOSIS for domain A5

ID	A.5 Information security policies
Risk 1	5-Medium
Risk 6	7-Very high
Risk 8	6-High
Risk 10	4-Low Medium
Risk 13	8-Important
Risk 14	8-Important
Risk 16	5-Medium
Risk 17	5-Medium
Risk 18	7-Very high
Risk 20	7-Very high
Risk 22	7-Very high
Risk 23	7-Very high

With information captured (step 9), then risks were pairwise compared to each other using Table 4 with respect to each domain in SD (step 10). The same was done for domains with respect to each risk (as in step 4 for goals and domains). Because this is done with SD, a manual table similar with Table 13 is not provided, but pairwise comparison done in SD is shown in Figure 7. More of these comparisons can be found in section A.1 in Appendix. As outlined in step 11, domains are fully compared regarding risks and risks fully compared regarding domains.

Step 12A, using as input, the output from 6B, 6C, 11A and 11B is used in SD to apply ANP as described in research design Figure 3. Finally, in step 13 we had results of information security risks based on strategic goals.

3.4 Validity and Reliability

As mentioned in section 2.1.3, the validity and reliability of AHP and ANP relies on a value of inconsistency less than 0.1, although several studies question validity of results based on a 0.1 value on inconsistency [19], [74]. In addition to other projects and studies that have been using AHP and ANP, value 0.1 proposed by Saaty has been backed up from other studies and these serve as our validation grounds for the thesis [75], [4], [35].

In addition, the opinion of the ISM of the use case organization is required to discuss about findings of the method proposed.

3.5 Super Decisions Software

For this study, Super Decisions 2.10 software for Windows was used over Expert Choice and other online calculators since the first one is suitable for both AHP and ANP and provides a free trial for personal use.[4]. Below there are some screenshots of the use case in the software.

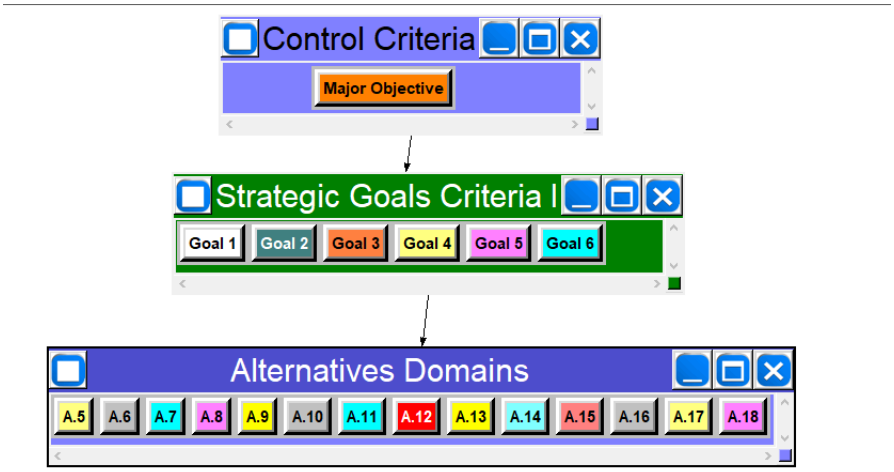

Figure 4. The model in SuperDecisions-AHP

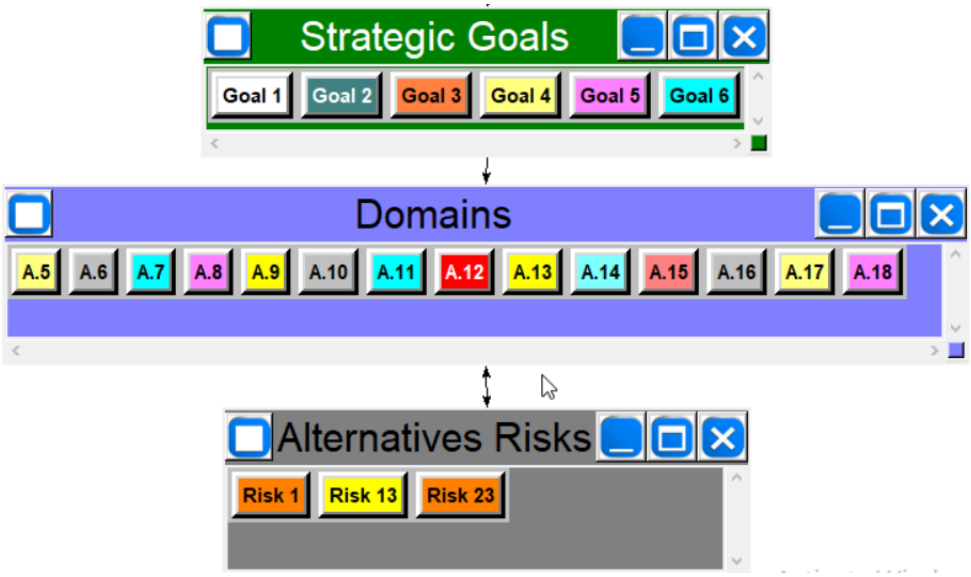

Figure 5. The model in SuperDecisions-ANP

The full model looks as shown in Figure 6.

[4]At the time of the study SD 3.2 in Beta version was available but it proved to be unstable and would crash often.

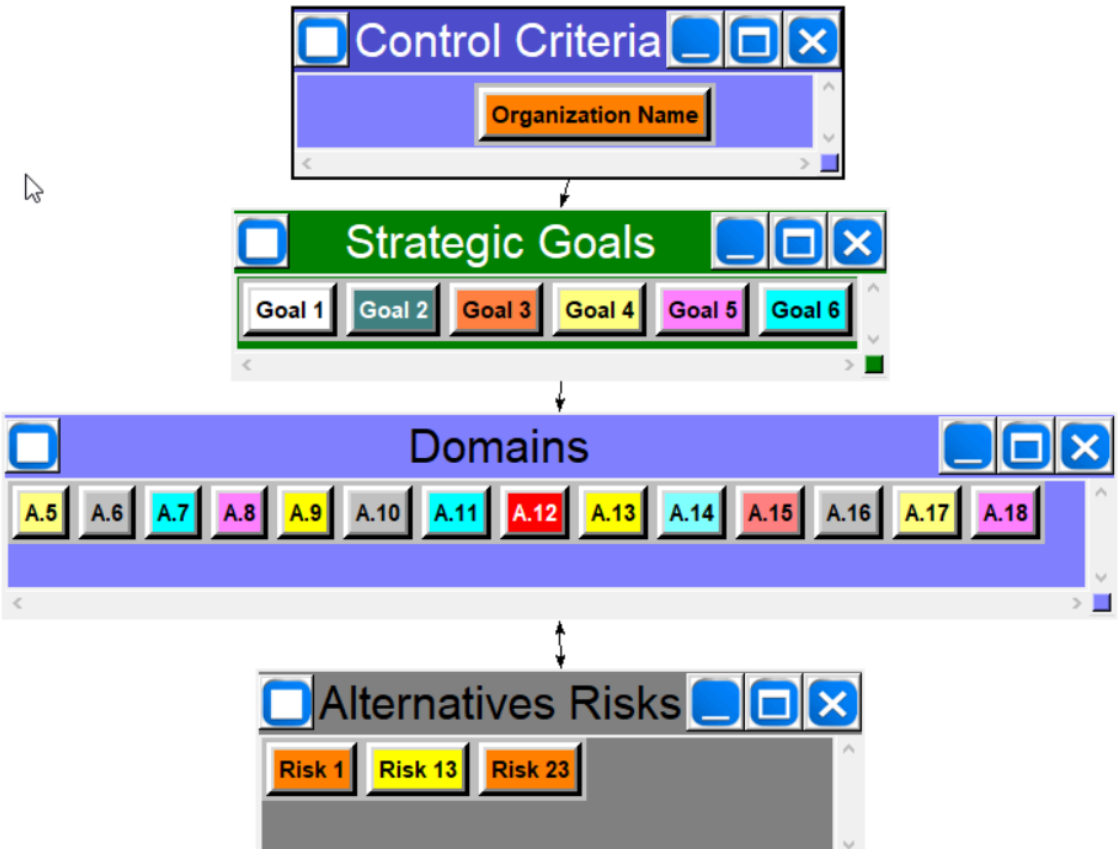

Figure 6. The model in SuperDecisions-AHP/ANP

Figure 7 shows pairwise comparison between goals with respect to the organization (step 5A) and on the right is given goal ranking (corresponds with 6B in Figure 3).

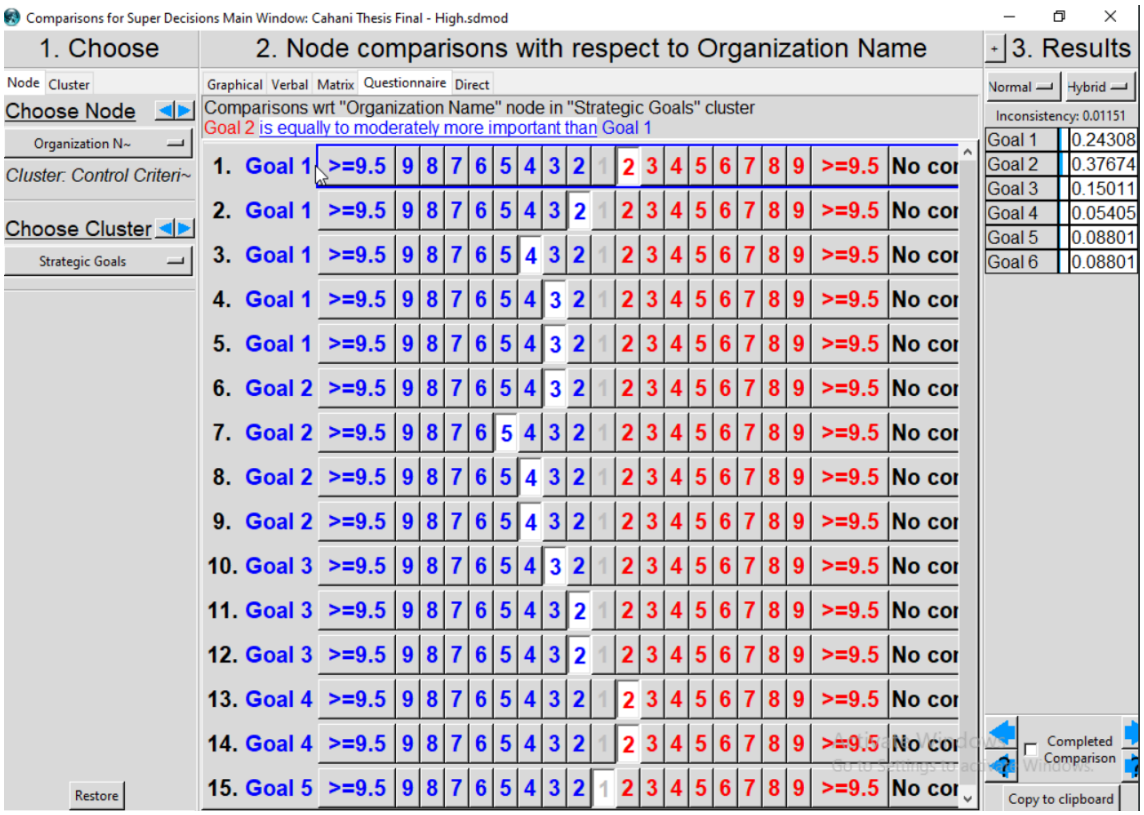

Figure 7. Goal comparison in SD for organization

Figure 8 shows ranking results for high risks. Column Total shows percentage out of all domains and other risks, normal column shows percentage of each risk compared only with that group of risks while Ideal column sets the highest risk with value 1 and the rest are given as a ratio of the highest risk value. Ranking column gives ranking of these goals.

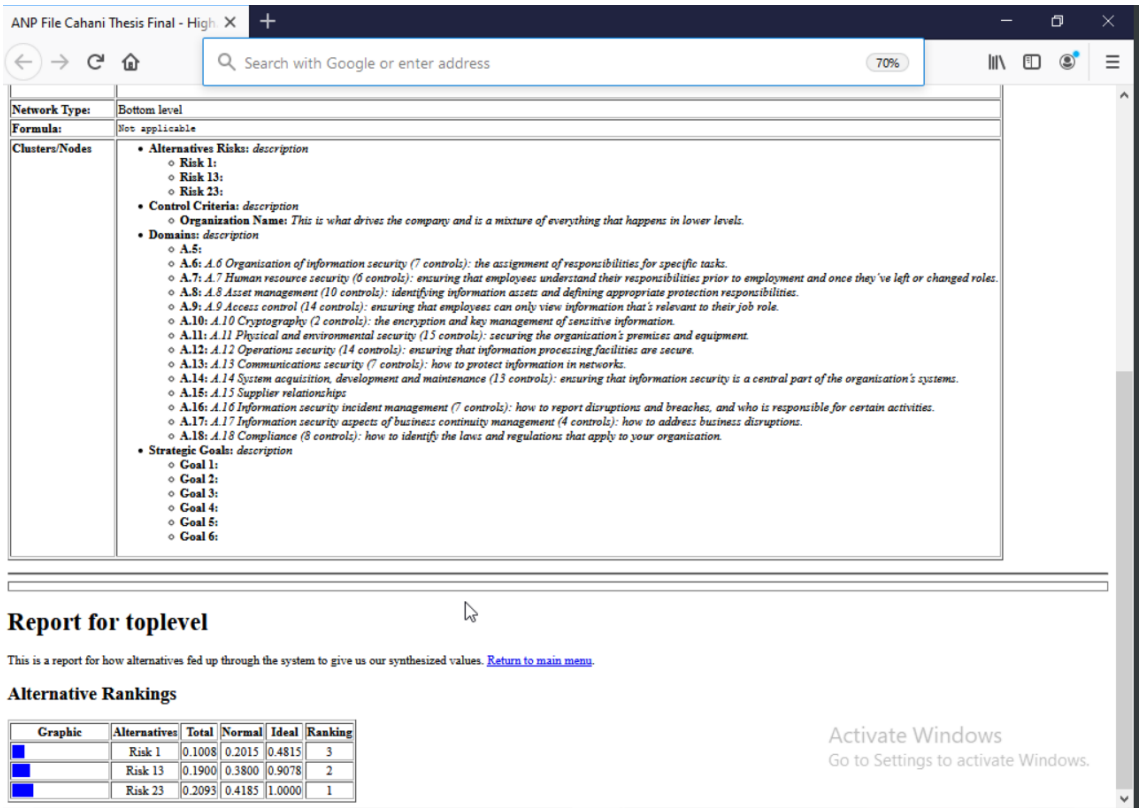

Figure 8. Ranking for high risks-Use Case Organization

4. Use Case Organization and Results

This chapter gives background information about the use case organization in the study, introduces the reader with strategic goals and risks identified and analyse results that come after applying the proposed method by elaborating in major findings.

4.1 Use case organization

The use case organization of this thesis operates finance industry. Company is divided in teams/departments of: executive team, IT, customer support, marketing, compliance, HR and finance. Being a company that relies in information technology for its activity, the organization is exposed to IT risks and therefore is crucial to be compliant and follow best practices in order to securely keep business operations running. The organization has to comply with various legislation and information security standards which for confidentiality reasons will not be mentioned in this thesis.

In total, a list of six strategic goals identified and set from executive team (here represented by CEO) was provided are identified from Goal 1 to Goal 6.

The list of risks identified from information security manager are identified as risks followed by a number ID as Risk 1, Risk 6, Risk 8, Risk 10, Risk 13, Risk 14, Risk 16, Risk 17, Risk 18, Risk 20, Risk 22 and Risk 23. Risks in the list were not solely identified for the purpose of this thesis. Therefore the missing ones, had already been treated (accepted, shared or transferred) and were not part of our study.

4.2 Results

4.2.1 Use case organization strategic goals

Domain mapping for strategic goals

Identified goals in step 1 and mapping into domains done in step 2, give results for relationships that each strategic goal has with each domain (step 3 in Figure 3). After pairwise comparison in step 4, the outcome is domain pairwise comparisons with respect

to goals. Chart in Figure 9 gives the results of domains ranked per Goal 1.

The rest of results can be found in Appendix section A.4.1.

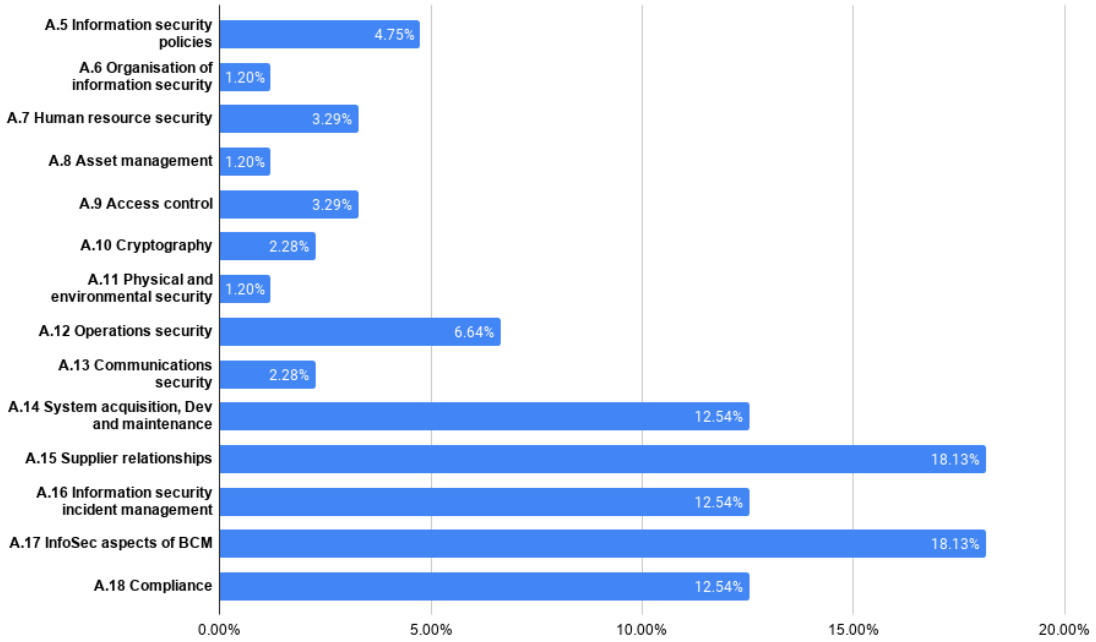

Figure 9. Domain Mapping per Goal 1

After doing pairwise comparison step 4 (also shown manually done in Table 13), its result is goals ranked (6B) with respect to the whole organization (6A) and domains globally ranked (6C) based on relationship they have with goals in 6B (refer to Figure 3 and 4). Results for goal ranking are shown in the chart in Figure 10. This ranking is expected, as in pairwise comparison Goal 2 and Goal 1 dominate over the other goals (Table 13).

SD gives in step 6C, also domains ranked globally (6C) with respect only to goals (6B). Chart in Figure 11, reflects ranking aggregation for domains based on the importance that goals have, when AHP has been used (refer to Figure 3).

The three most important domains result to be A.18 Compliance, followed by A.17 Information security aspects of business continuity management and A.15 Supplier relationships. This is expected and consistent with information in Table 19 section A.4.1, as these domains have been assigned a very high importance for the three most important goals.

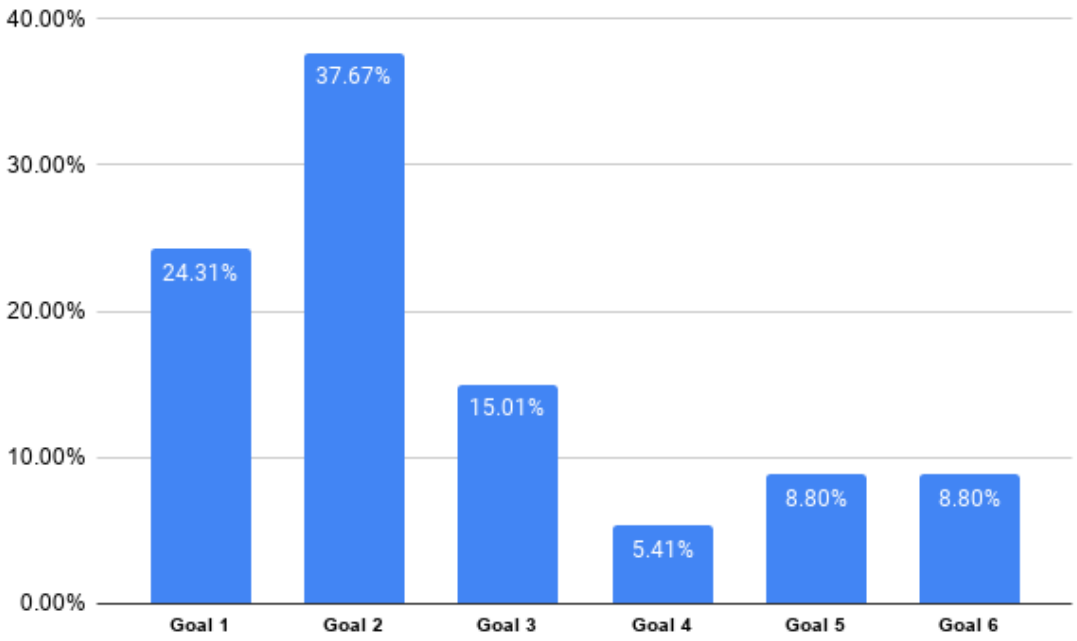

Figure 10. Strategic Goal Ranking (6B)

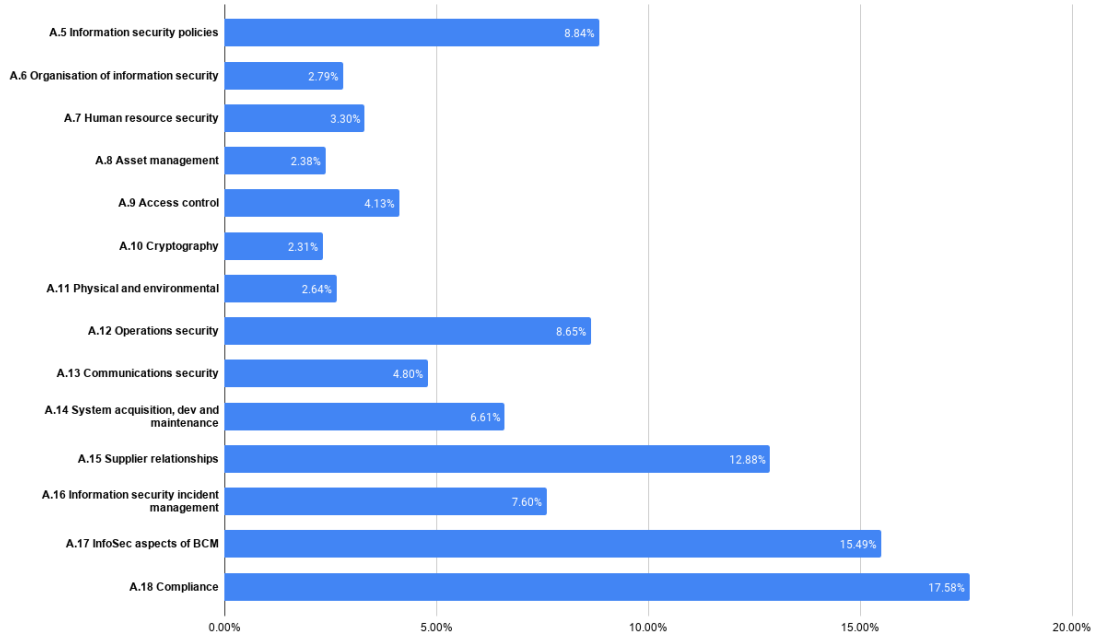

Figure 11. Global Ranking for Domains based only in goals (6C)

4.2.2 Use case organization risk results

Information security risks identified in step 7 and mapped with domains in step 8, provide the necessary information risks and domains in step 9. As mentioned in section 3.1 steps 7 to 13 need to be repeated for every level of risk. Following is given the example for high risks but procedure is the same for medium and low level.

Table 17, shows the information for Risk 1. According to evaluation given from ISM, this risk concerns the most domain A.13 Communications security and A.16 Information security incident management. The rest of domain mapping for each risk, can be found in Table 20 and Table 21 in Appendix.

Table 17. Domain mapping for Risk 1

Name of domain	**Level of importance (step 8)**	**Pairwise comparison % (step 9)**
A.5 Information security policies	5-Medium	8.47%
A.6 Organisation of information security	1-Minor/No importance	2.04%
A.7 Human resource security	1-Minor/No importance	2.04%
A.8 Asset management	1-Minor/No importance	2.04%
A.9 Access control	1-Minor/No importance	2.04%
A.10 Cryptography	6-High	11.72%
A.11 Physical and environmental security	1-Minor/No importance	2.04%
A.12 Operations security	7-Very high	16.27%
A.13 Communications security	8-Important	22.49%
A.14 System acquisition, Dev and maintenance	1-Minor/No importance	2.04%
A.15 Supplier relationships	1-Minor/No importance	2.04%
A.16 Information security incident management	7-Very high	16.27%
A.17 InfoSec aspects of BCM	1-Minor/No importance	2.04%
A.18 Compliance	5-Medium	8.47%

Information for domains regarding risks, is collected in step 8 and Table 18 shows the importance that each risk has for domain A.5 Information security policies. Values in % are product of applying pairwise comparison in step 10. In addition, the inconsistency rate of 1.76% shows that results are also reliable.

Table 18. Risk mapping for A.5 Information security policies

ID A.5 Information security policies	**Importance**	**In %**
Risk 1	5-Medium	12.20%
Risk 13	8-Important	55.84%
Risk 23	7-Very high	31.96%

All other results for domain pairwise comparisons with respect to risks (11A) and information security risks pairwise comparisons with respect to domains (11B) can be found in Table 20 and Table 21 in Appendix.

After applying ANP as described in step 12, using results for goals ranked in Figure 10, domains ranked in 6C and pairwised in 11A and information security risks pairwised in 11B in final step results are as shown in Figure 12.

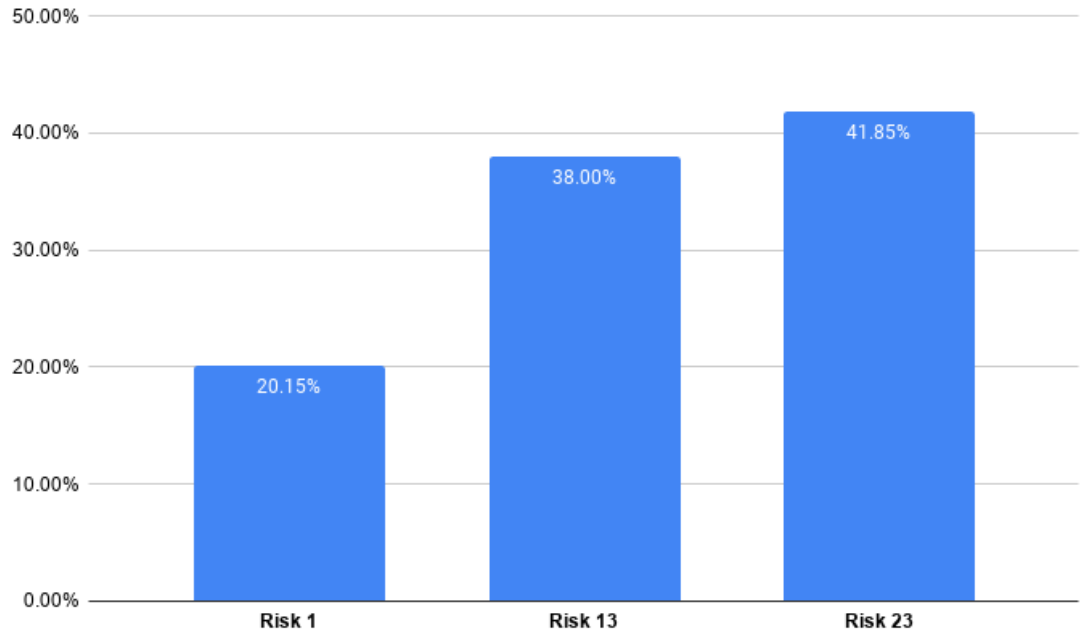

Figure 12. High Risks Ranking (step 13)

Following are interpretations about high, medium and low risk risk results based on AHP and ANP principles.

Ranking of high level risks

Risk 13 and Risk 23 are ranked first due to strong relationship for domains A.18 Compliance, A.5 Information security policies and A.12 Operations security (refer to Table A.4.2 and the importance that these domains have on top three goals (refer to Table 19). Risk 23 is ranked higher than Risk 13, due to stronger relationship with domain A.17 Information security aspects of business continuity management (ranked 2nd among domains) that is strongly related with Goal 2 (ranked 1st). Also, Risk 23 has a strong relationship with domain A.15 Supplier relationships which from the other side is strongly related with Goal 1 (ranked 2nd among goals). Risk 1 is ranked lowest in this group because domains that it concerns in a high importance are few (refer to section A.4.2) and these domains are

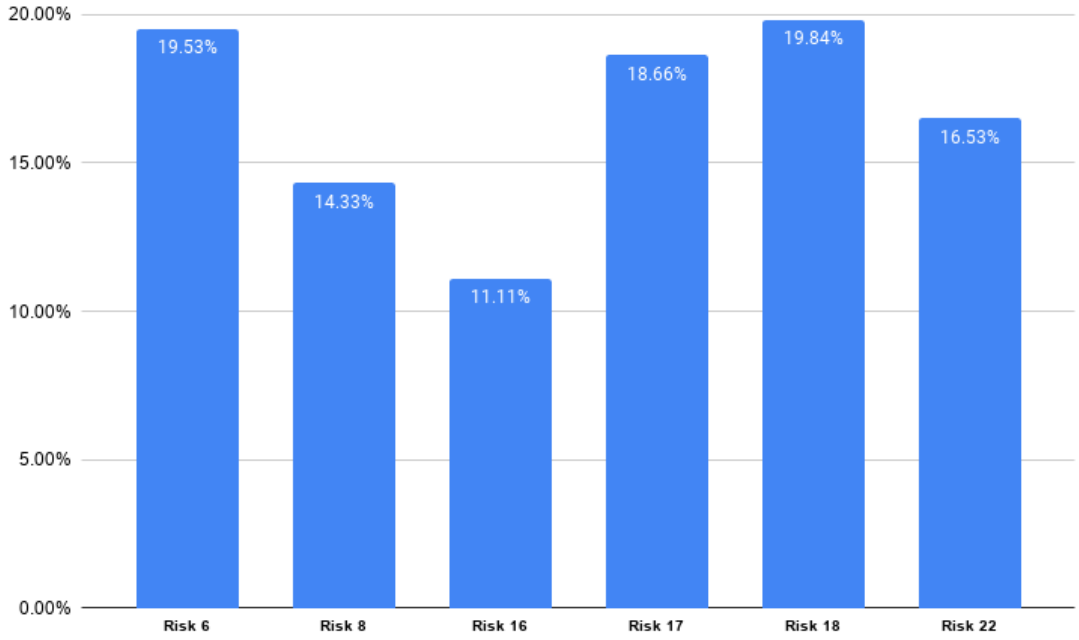

Figure 13. Medium Risks Ranking (Step 13)

mainly important for goals ranked low (Goal 6).

Ranking of medium level risks

According to results for medium risks shown in chart given in Figure 13, Risk 6, Risk 17 and Risk 18 are the three most important risks of this group. This comes due to their relationships with five most important domains: A.5 Information security policies, A.12 Operations security, A.15 Supplier relationships, A.17 Information security aspects of business continuity management and A.18 Compliance, which from the other side are given a very high importance for Goal 1 (ranked 2nd), Goal 2 (ranked 1st) and Goal 3 (ranked 3rd). Furthermore, Risk 18 is ranked the highest in medium risk group compared to Risk 6 because it has a stronger connection with domain A.17 Information security aspects of business continuity management (ranked 2nd among domains) as shown in Figure 11. This domain plays a very important role for all three most important goals identified for the organization (Figure 10). This is consistent with expectations from AHP and ANP relationships created between strategic goals, domains and risks. Other risks are ranked lower as a result of weaker relationships with main domains (Risk 22) or domains that concern relatively low ranked goals (Risk 8).

Ranking of low level risks

Results for low level risks shown in Figure 14, rank Risk 14 as the most important of this

group. Although this risk and Risk 20, have similar level of relationship with domains A.17 Information security aspects of business continuity management and A.18 Compliance, Risk 14 is ranked higher than Risk 20 due to its relationship with domain A.15 Supplier relationships which is very important for five goals (refer to Table 19). Risk 10 is least important of this group because the domains that is related are mostly important only for Goal 5, which is one of least important goals for the organization.

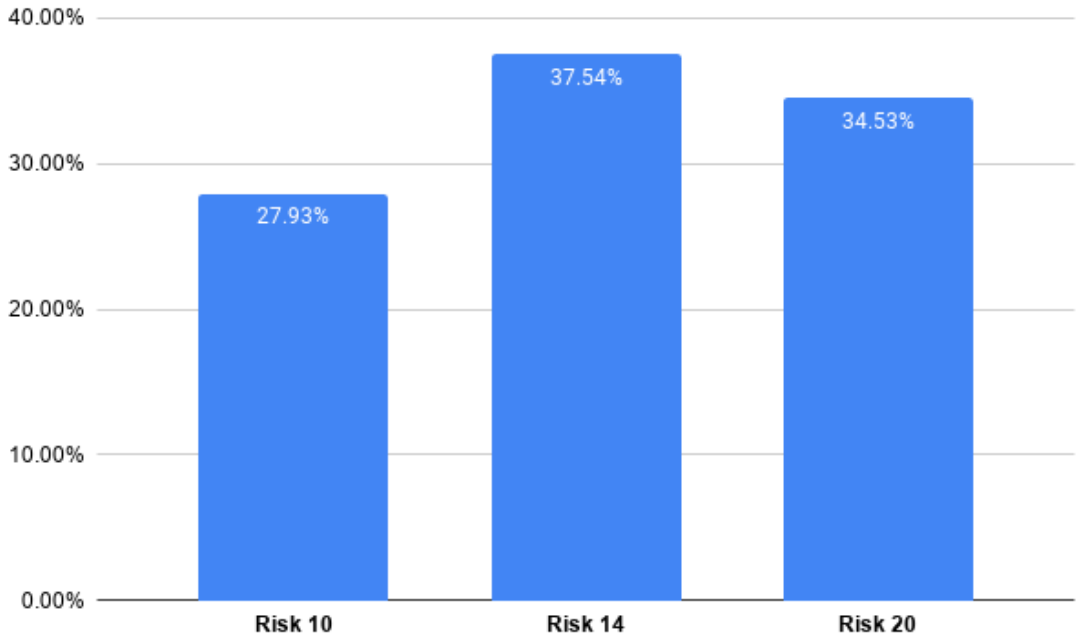

Figure 14. Low Risks Ranking (Step 13)

5. Discussions

This study discussed and dealt with an important aspect that information security teams face on prioritizing their work, while ensuring that they are also supporting strategic goals. Gaps identified in previous studies in literature review were taken into consideration, addressed carefully and a method was proposed.

Results from use case showed that risks can be ranked based on strategic goals, reflecting relationships on common domains when AHP and ANP is used. Risks previously labelled with the same level, can be set apart based on the relations that have with identified strategic goals. Use case also showed that risks connected relatively with the same domains, by the same or approximate importance, will also provide approximate results consistent with what is expected from methodologies. However, study could not show if there is a limit number of risks that can be taken into analysis and what this limit could be. Besides, time has not been taken into study as a factor and treats all risks in the same group with the same sense of urgency. Despite the number of risks in use case was relatively small, study showed that they can be well differentiated from each other as Risk 1 in Figure 12, Risk 16 in Figure 13 or Risk 10 in Figure 14, when compared to other risks of the same group.

It would be very interesting to see how this methodology would work in other organizations of a bigger size and companies in other industries, which face information security risks in a much higher frequency. AHP and ANP allow to include more elements in their model, so it would be of high interest to see if cost benefit analysis can be integrated. I would encourage to see new methodologies that would tackle the same problem and compare findings. Worth considering is also, how the method would handle when a very large number of risks would emerge but that requires a much profound study and more aspects to be included in the study. Because SD used requires an extensive data entry, I would be very eager to see in the future a software or service that can integrate strategic goals and information security risks and align them together.

6. Summary

In this thesis, I brought up an approach that would prioritize information security risks by reflecting strategic goals of the organization. This methodology helps information security teams to identify common domains with those of decision makers and adjust their priorities, without shifting their focus from risk management. Regardless the subjective nature that its needed when putting it into practice, if these two subjects, domain relationships that associate them, are well understood and there is a thorough active involvement of stakeholders, connecting them together becomes easier. The study proved that results of using AHP and ANP methodologies reflect the reality and meet expectations of information security manager. In addition as ISM of the use case organization points out : *"we have finite resources to implement these treatments"*, therefore, it is a necessity to have risks aligned, so that available resources as used in an optimal way.

By using the methodology proposed in this thesis, it is possible to bring in together aspects that concern not only one project or a certain field, but an entire organization by keeping the balance between information technology aspects concerning information security team and that of business, concerning decision makers. The first step has been made and although the initial process might take time to implement, its benefits can be enormous and information security risk management can be very supportive instead of being a burden for the organization.

I am confident that once this methodology will be used in other cases, it will be improved then it will be very helpful to set priorities for information security teams.

Bibliography

[1] Etishree Agarwal et al. “Delineation of groundwater potential zone: An AHP/ANP approach”. In: *Journal of earth system science* 122.3 (2013), pp. 887–898.

[2] Mohammed I Al Khalil. “Selecting the appropriate project delivery method using AHP”. In: *International journal of project management* 20.6 (2002), pp. 469–474.

[3] Mojtaba Amiri, Mahmoud Reza Asadi, and Fatemeh Delbari Ragheb. “Identification and ranking effective factors on the internet shopping use of Fuzzy ANP”. In: *Iranian Business Management* 3.7 (2011), pp. 37–92.

[4] B Apostolou and JM Hassell. “Note on consistency ratio: a reply”. In: *Mathematical and computer modelling* 35.9-10 (2002), pp. 1081–1083.

[5] Pablo Aragonés-Beltrán et al. “An AHP (Analytic Hierarchy Process)/ANP (Analytic Network Process)-based multi-criteria decision approach for the selection of solar-thermal power plant investment projects”. In: *Energy* 66 (2014), pp. 222–238.

[6] AXELOS. *ITIL Foundation, ITIL 4 edition*. ITIL®. AXELOS Limited, 2019. ISBN: 9780113316076. URL: https://www.axelos.com/store/book/itil-foundation-itil-4-edition.

[7] Dennis Baker et al. *Guidebook to decision-making methods*. Tech. rep. WSRC-IM-2002-00002, Department of Energy, USA, 2002.

[8] Ozden Bayazit. “Use of AHP in decision-making for flexible manufacturing systems”. In: *Journal of Manufacturing Technology Management* (2005).

[9] Ozden Bayazit. “Use of analytic network process in vendor selection decisions”. In: *Benchmarking: An International Journal* (2006).

[10] Jarosław Becker et al. “ANP-based analysis of ICT usage in Central European enterprises”. In: *Procedia computer science* 126 (2018), pp. 2173–2183.

[11] Alfred Dupont Chandler. *Strategy and structure: Chapters in the history of the industrial enterprise*. Vol. 120. MIT press, 1990.

[12] Dimitris E Charilas et al. “Application of fuzzy AHP and ELECTRE to network selection”. In: *International Conference on Mobile Lightweight Wireless Systems*. Springer. 2009, pp. 63–73.

[13] Ching-Hsue Cheng. “Evaluating naval tactical missile systems by fuzzy AHP based on the grade value of membership function”. In: *European journal of operational research* 96.2 (1997), pp. 343–350.

[14] Ching-Hsue Cheng, Kuo-Lung Yang, and Chia-Lung Hwang. “Evaluating attack helicopters by AHP based on linguistic variable weight”. In: *European journal of operational research* 116.2 (1999), pp. 423–435.

[15] Eddie WL Cheng and Heng Li. “Application of ANP in process models: An example of strategic partnering”. In: *Building and environment* 42.1 (2007), pp. 278–287.

[16] Eddie WL Cheng and Heng Li. “Information priority-setting for better resource allocation using analytic hierarchy process (AHP)”. In: *Information Management & Computer Security* (2001).

[17] Eddie WL Cheng, Heng Li, and Ling Yu. “The analytic network process (ANP) approach to location selection: a shopping mall illustration”. In: *Construction Innovation* 5.2 (2005), pp. 83–98.

[18] Ta-Chung Chu. “Facility location selection using fuzzy TOPSIS under group decisions”. In: *International journal of uncertainty, fuzziness and knowledge-based systems* 10.06 (2002), pp. 687–701.

[19] Peter Chu and John Kuang-Han Liu. “Note on consistency ratio”. In: *Mathematical and Computer Modelling* 35.9-10 (2002), pp. 1077–1080.

[20] Shu-Hsing Chung, Amy HI Lee, and Wen-Lea Pearn. “Analytic network process (ANP) approach for product mix planning in semiconductor fabricator”. In: *International journal of production economics* 96.1 (2005), pp. 15–36.

[21] *COBIT 2019 FRAMEWORK: INTRODUCTION & METHODOLOGY*. Standard. IL, USA: ISACA Information Systems Audit and Control Association, Oct. 2019.

[22] Committee of Sponsoring Organizations of the Treadway Commission COSO. *Enterprise Risk Management Integrating with Strategy and Performance*. 2017. URL: https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf (visited on 02/23/2020).

[23] Jose Luis De La Vara et al. “COMPRO: a methodological approach for business process contextualisation”. In: *OTM Confederated International Conferences" On the Move to Meaningful Internet Systems"*. Springer. 2010, pp. 132–149.

[24] Rubén Dorado et al. “An AHP application to select software for engineering education”. In: *Computer Applications in Engineering Education* 22.2 (2014), pp. 200–208.

[25] Steven Finch. “Transitive relations, topologies and partial orders”. In: *unpublished note* (2003).

[26] Joseph M Firestone. “Enterprise information portals and knowledge management”. In: Routledge, 2003, p. 56.

[27] Masoud Rahiminezhad Galankashi et al. “Prioritizing green supplier selection criteria using fuzzy analytical network process”. In: *Procedia CIRP* 26.2015 (2015), pp. 689–694.

[28] Ali Görener. “Comparing AHP and ANP: an application of strategic decisions making in a manufacturing company”. In: *International Journal of Business and Social Science* 3.11 (2012).

[29] Charles H Granger. *The hierarchy of objectives*. Vol. 42. 3. Harvard Business Review.

[30] John D Hamshere. “Regressing Domesday Book: tax assessments of Domesday England”. In: *The Economic History Review* 40.2 (1987), pp. 247–251.

[31] C Derrick Huang and Qing Hu. “Achieving IT-business strategic alignment via enterprise-wide implementation of balanced scorecards”. In: *Information Systems Management* 24.2 (2007), pp. 173–184.

[32] IBM IBM Global Technology Service. *Aligning IT risk management with strategic business goals*. 2014. URL: https://www.ibm.com/downloads/cas/PMNWONX9 (visited on 01/19/2020).

[33] Syamsuddin Irfan and Hwang Junseok. “The use of AHP in security policy decision making: an open office calc application”. In: *Journal of Software* 5.2 (2010), pp. 1162–1169.

[34] Alessio Ishizaka. “Clusters and pivots for evaluating a large numberof alternatives in AHP”. In: *Pesquisa Operacional* 32.1 (2012), pp. 87–102.

[35] Alessio Ishizaka and Sajid Siraj. “Are multi-criteria decision-making tools useful? An experimental comparative study of three methods”. In: *European Journal of Operational Research* (May 2017). DOI: 10.1016/j.ejor.2017.05.041.

[36] *ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary*. Standard. Geneva, CH: International Organization for Standardization, Feb. 2018.

[37] *ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements*. Standard. Geneva, CH: International Organization for Standardization, Oct. 2013.

[38] The International Organization for Standardization ISO. *ISO 31000:2018(en) Risk management — Guidelines*. ISO 31000: Enterprise Risk Management. Certified Enterprise Risk Manager (R) Academy (2018), 2018. ISBN: 9780965466516. URL: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en.

[39] Wyn Jenkins and Dave Williamson. *Strategic management and business analysis*. Routledge, 2015.

[40] Shireesha Katam, Pavol Zavarsky, and Francis Gichohi. "Applicability of domain based security risk modeling to scada systems". In: *2015 World Congress on Industrial Control Systems Security (WCICSS)*. IEEE. 2015, pp. 66–69.

[41] Allen Kent and James G Williams. *Encyclopedia of Microcomputers: Volume 26-Supplement 5*. CRC press, 2000.

[42] Navid Khademi, Kambiz Behnia, and Ramin Saedi. "Using analytic hierarchy/network process (AHP/ANP) in developing countries: shortcomings and suggestions". In: *The Engineering Economist* 59.1 (2014), pp. 2–29.

[43] Vincent S Lai, Bo K Wong, and Waiman Cheung. "Group decision making in a multiple criteria environment: A case using the AHP in software selection". In: *European Journal of Operational Research* 137.1 (2002), pp. 134–144.

[44] Abbas Mardani et al. "Multiple criteria decision-making techniques and their applications–a review of the literature from 2000 to 2014". In: *Economic Research-Ekonomska Istraživanja* 28.1 (2015), pp. 516–571.

[45] Daniel L Moody and Peter Walsh. "Measuring the Value Of Information-An Asset Valuation Approach." In: *ECIS*. 1999, pp. 496–512.

[46] Pedro Mota, Ana Rita Campos, and Rui Neves-Silva. "First look at MCDM: Choosing a decision method". In: *Advances in Smart Systems Research* 3.1 (2012), p. 25.

[47] Nolberto Munier. "300-Tool for selecting the most appropriate MCDM method to solve a problem". In: (2019).

[48] Shin-ichi Ohnishi et al. "A weights representation for absolute measurement AHP using fuzzy sets theory". In: *2011 5th International Symposium on Computational Intelligence and Intelligent Informatics (ISCIII)*. IEEE. 2011, pp. 67–70.

[49] OpenGroup. *Business Process Domain Views*. 2006. URL: https://pubs.opengroup.org/architecture/togaf8-doc/arch/chap33.html (visited on 04/12/2020).

[50] Juan-Pascual Pastor-Ferrando et al. "An ANP-and AHP-based approach for weighting criteria in public works bidding". In: *Journal of the Operational Research Society* 61.6 (2010), pp. 905–916.

[51] Leandro Pecchia et al. “Analytic hierarchy process (AHP) for examining healthcare professionals’ assessments of risk factors”. In: *Methods of information in medicine* 50.05 (2011), pp. 435–444.

[52] Selcuk Percin. “Using the ANP approach in selecting and benchmarking ERP systems”. In: *Benchmarking: An International Journal* (2008).

[53] Eleni Philippou, Sylvain Frey, and Awais Rashid. “Contextualising and Aligning Security Metrics and Business Objectives: a GQM-based Methodology”. In: *Comput. Secur.* 88 (2019).

[54] Valentinas Podvezko and Henrikas Sivilevičius. “The use of AHP and rank correlation methods for determining the significance of the interaction between the elements of a transport system having a strong influence on traffic safety”. In: *Transport* 28.4 (2013), pp. 389–403.

[55] R Ramanathan. “A note on the use of the analytic hierarchy process for environmental impact assessment”. In: *Journal of environmental management* 63.1 (2001), pp. 27–35.

[56] R Ramanathan and LS Ganesh. “Using AHP for resource allocation problems”. In: *European Journal of Operational Research* 80.2 (1995), pp. 410–417.

[57] Rapid7. *Information Security Risk Management*. 2016. URL: https://www.rapid7.com/fundamentals/information-security-risk-management/ (visited on 03/29/2020).

[58] Harvard Business Review. *Crafting Strategy - Strategic planning*. 1987. URL: https://hbr.org/1987/07/crafting-strategy (visited on 05/09/2020).

[59] Roseanna W Saaty. “The analytic hierarchy process—what it is and how it is used”. In: *Mathematical modelling* 9.3-5 (1987), pp. 161–176.

[60] Thomas L Saaty. “Absolute and relative measurement with the AHP. The most livable cities in the United States”. In: *Socio-Economic Planning Sciences* 20.6 (1986), pp. 327–331.

[61] Thomas L Saaty. “Decision making with the analytic hierarchy process”. In: *International journal of services sciences* 1.1 (2008), pp. 83–98.

[62] Thomas L Saaty. “Decision making—the analytic hierarchy and network processes (AHP/ANP)”. In: *Journal of systems science and systems engineering* 13.1 (2004), pp. 1–35.

[63] Thomas L Saaty. “Fundamentals of the analytic network process”. In: *Proceedings of the 5th international symposium on the analytic hierarchy process*. 1999, pp. 12–14.

[64] Thomas L Saaty. “Making and validating complex decisions with the AHP/ANP”. In: *Journal of Systems Science and Systems Engineering* 14.1 (2005), pp. 1–36.

[65] Thomas L Saaty. “Time dependent decision-making; dynamic priorities in the AHP/ANP: Generalizing from points to functions and from real to complex variables”. In: *Mathematical and Computer Modelling* 46.7-8 (2007), pp. 860–891.

[66] Thomas L Saaty and Luis G Vargas. “The analytic network process”. In: *Decision making with the analytic network process*. Springer, 2013, pp. 1–40.

[67] Thomas Saaty and Konrad Kułakowski. “Axioms of the analytic hierarchy process (ahp) and its generalization to dependence and feedback: the analytic network process (ANP)”. In: *arXiv preprint arXiv:1605.05777* (2016).

[68] Carlos Perez Sanchez and Pablo Solar Vilariño. *PHP Microservices*. Packt Publishing Ltd, 2017.

[69] Michael Schermann et al. “Information technology risks: An interdisciplinary challenge”. In: *Risk-A Multidisciplinary Introduction*. Springer, 2014, pp. 387–405.

[70] Joseph Steinberg. *Official (ISC) 2 Guide to the CISSP-ISSMP CBK*. CRC Press, 2015.

[71] Paul P Tallon and Kenneth L Kraemer. “Investigating the relationship between strategic alignment and information technology business value: the discovery of a paradox”. In: *Creating business value with information technology: Challenges and solutions*. IGI Global, 2003, pp. 1–22.

[72] Evangelos Triantaphyllou. “Multi-criteria decision making methods”. In: *Multi-criteria decision making methods: A comparative study*. Springer, 2000, pp. 5–21.

[73] Andrew P. Vayda. “Progressive contextualization: Methods for research in human ecology”. In: (1983), pp. 265–281.

[74] William C Wedley. “Consistency prediction for incomplete AHP matrices”. In: *Mathematical and Computer Modelling* 17.4-5 (1993), pp. 151–161.

[75] Diederik JD Wijnmalen. “Analysis of benefits, opportunities, costs, and risks (BOCR) with the AHP–ANP: A critical validation”. In: *Mathematical and computer modelling* 46.7-8 (2007), pp. 892–905.

[76] Carla L Wilkin and Robert H Chenhall. “A review of IT governance: A taxonomy to inform accounting information systems”. In: *Journal of Information Systems* 24.2 (2010), pp. 107–146.

[77] Yoram Wind and Thomas L Saaty. “Marketing applications of the analytic hierarchy process”. In: *Management science* 26.7 (1980), pp. 641–658.

[78] Li Yan and Li Xiansheng. “Study on ANP cluster supply chain risk evaluation”. In: *2010 International Conference on Logistics Systems and Intelligent Management (ICLSIM)*. Vol. 3. IEEE. 2010, pp. 1296–1299.

[79] Chang-Lin Yang, Shan-Ping Chuang, and Rong-Hwa Huang. “Manufacturing evaluation system based on AHP/ANP approach for wafer fabricating industry”. In: *Expert Systems with Applications* 36.8 (2009), pp. 11369–11377.

[80] Yu-Ping Ou Yang, How-Ming Shieh, and Gwo-Hshiung Tzeng. “A VIKOR technique based on DEMATEL and ANP for information security risk control assessment”. In: *Information Sciences* 232 (2013), pp. 482–500.

[81] Ali Yavari et al. “Contaas: An approach to internet-scale contextualisation for developing efficient internet of things applications”. In: (2017).

[82] Selim Zaim et al. “Maintenance strategy selection using AHP and ANP algorithms: a case study”. In: *Journal of Quality in Maintenance Engineering* (2012).

[83] Xiaojing Zhao et al. “AHP-ANP–fuzzy integral integrated network for evaluating performance of innovative business models for sustainable building”. In: *Journal of Construction Engineering and Management* 143.8 (2017), p. 04017054.

A. Super Decisions and Reflections of ISM

A.1 Super Decisions

SD is a very useful tool when it comes to data entry because depending on user's preference and format on how data data/information is collected it can be entered in multiple ways. Figure 17 shows the matrix type of pairwise options that can be done for AHP and ANP using SD software, figure 18 shows the questionnaire pairwise comparison which is a more tedious work to do as the number of comparisons increases significantly with increasing number of alternatives (for n alternatives the number of comparisons is n(n-1)/2) but it tends to be more accurate when checking the inconsistency rate. Other comparisons modes are graphical (Figure 15), verbal (Figure 16) and direct (Figure 19.)

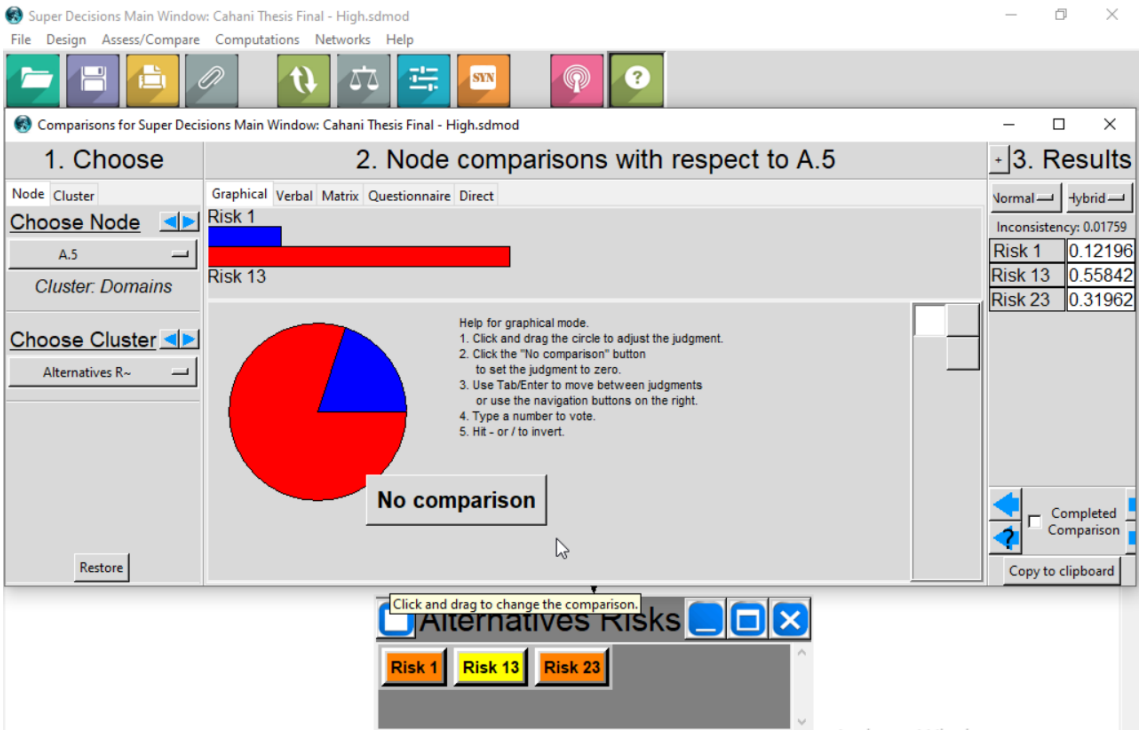

Figure 15. Graphical type pairwise-comparison in SuperDecisions

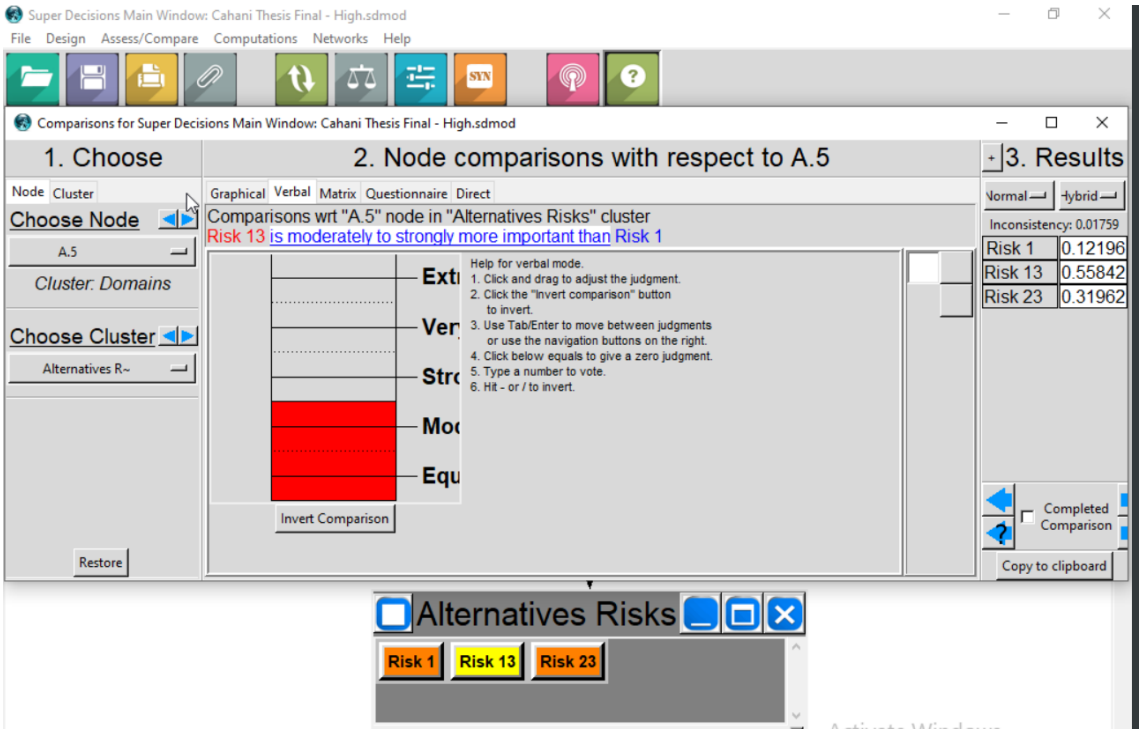

Figure 16. Verbal type pairwise-comparison in SuperDecisions

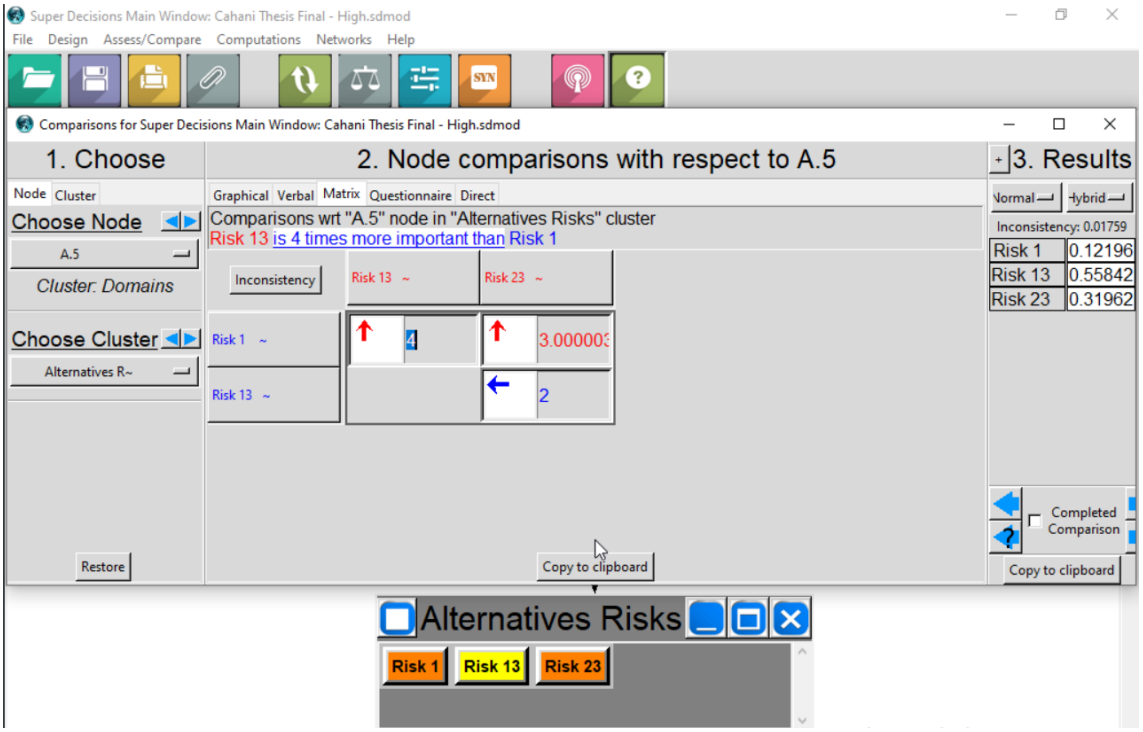

Figure 17. Matrix type pairwise-comparison in SuperDecisions

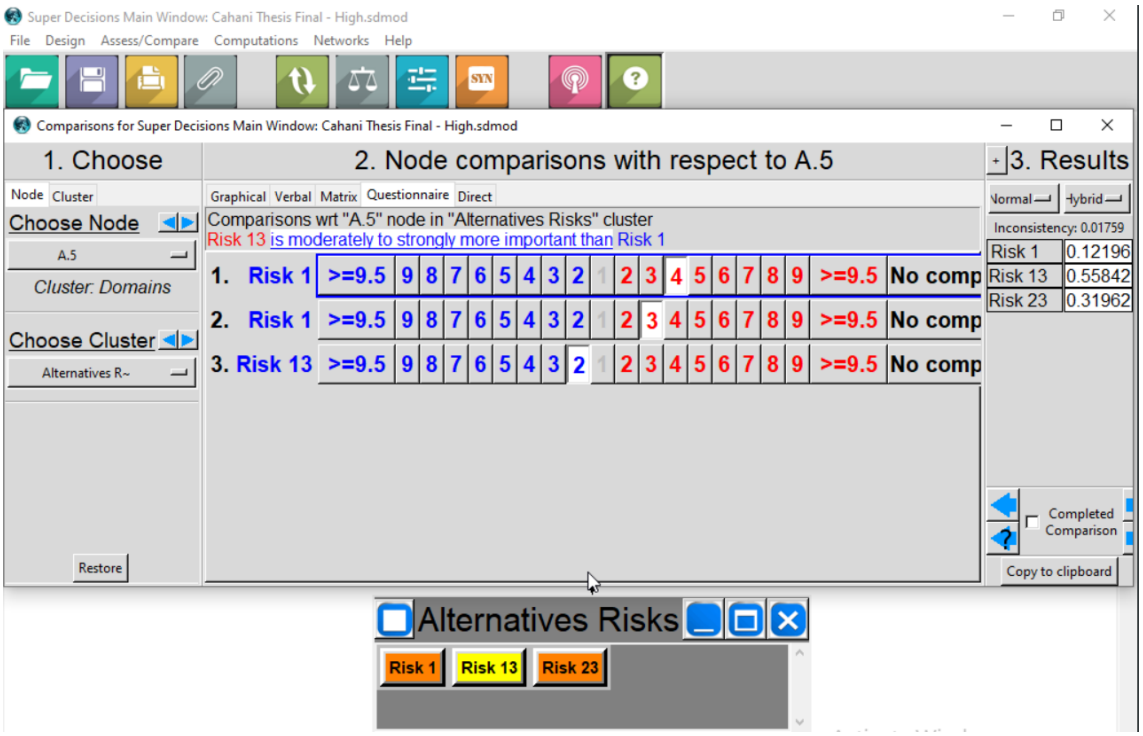

Figure 18. Questionnaire type pairwise-comparison in SuperDecisions

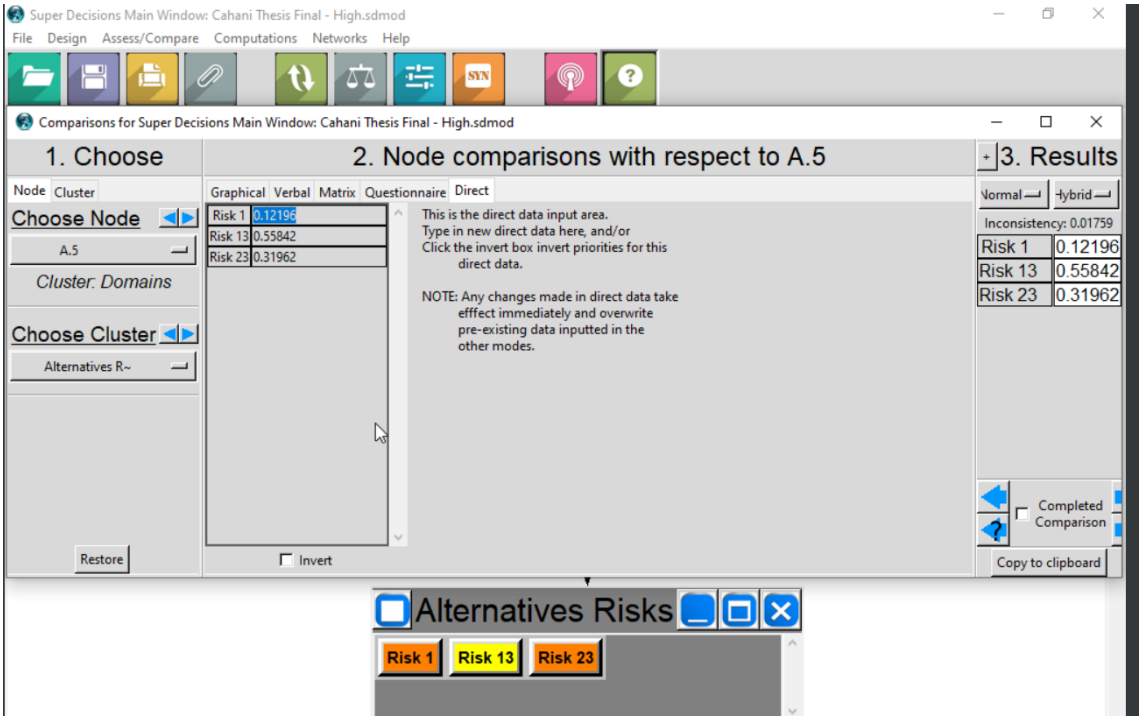

Figure 19. Direct type pairwise-comparison in SuperDecisions

A.2 Reflection of Information Security Manager of use case organization over the study

"I have had the opportunity to review the conclusions of Kadri Cahani's thesis study examining the relationship between Risk Management and Corporate Strategic Goal ranking. This study addresses a significant gap in business-oriented risk management. While traditional risk management allows the impacts of risks and their treatments to be quantified to a certain degree, it does not always provide useful guidance to prioritize these treatments. As the Information Security Manager, I was frequently called upon to prioritize risk treatment since we have finite resources to implement these treatments. Further, seeking executive support for particular risk treatment was made unnecessarily more difficult as traditional tools don't enable for an easy translation between risk and corporate strategic goals. Cahani's results in this study roughly coordinate with my intuitive expectations with respect to relative prioritization of risk treatments. Further, these results provide specific actionable guidance regarding the prioritization most likely to receive executive support. It would be interesting to see this model applied to larger organizations with a firmer understanding of their strategic goals. In addition, applying this model to organizations with more identified risks would provide a useful testbed for this evaluation model."

A.3 Use case organization strategic goals and risks

A.4 Domain mapping per goals and risks

Tables below give the information about mapping each domain per goal and risk. The values given in "Level of importance domain/goal" column are initial values given by stakeholders while "%" column are values that resulted after pairwise comparison.

A.4.1 Mapping domains with respect to each Goal

Mapping domains with respect to goals corresponds with step 2 in Figure 3.

Table 19. Domain Mapping Per Goal

Name of the goal	Domain Name	Level of importance domain/goal	%
Goal 2	A.5 Information security policies	6-High	12.17%
Goal 2- Inconsistency 2.86%	A.6 Organisation of information security	1-Minor/No importance	1.99%
	A.7 Human resource security	1-Minor/No importance	1.99%
	A.8 Asset management	1-Minor/No importance	1.99%
	A.9 Access control	1-Minor/No importance	1.99%
	A.10 Cryptography	1-Minor/No importance	2.63%
	A.11 Physical and environmental security	1-Minor/No importance	1.99%
	A.12 Operations security	6-High	12.17%
	A.13 Communications security	3-Low	4.76%
	A.14 System acquisition, Dev and maintenance	1-Minor/No importance	1.99%
	A.15 Supplier relationships	6-High	11.27%
	A.16 Information security incident management	3-Low	4.76%
	A.17 InfoSec aspects of BCM	7-Vey high	17.12%
	A.18 Compliance	8-Important	23.18%
Goal 3	A.5 Information security policies	6-High	6.07%
Goal 3- Inconsistency 1.93%	A.6 Organisation of information security	6-High	6.07%
	A.7 Human resource security	4-Low Medium	2.63%
	A.8 Asset management	5-Medium	3.85%
	A.9 Access control	7-Vey high	9.91%
	A.10 Cryptography	1-Minor/No importance	1.17%
	A.11 Physical and environmental security	1-Minor/No importance	1.17%
	A.12 Operations security	5-Medium	3.85%
	A.13 Communications security	5-Medium	3.85%
	A.14 System acquisition, Dev and maintenance	7-Vey high	9.91%
	A.15 Supplier relationships	7-Vey high	9.91%
	A.16 Information security incident management	7-Vey high	9.91%
	A.17 InfoSec aspects of BCM	7-Vey high	9.91%
	A.18 Compliance	9-Very important	21.79%
Goal 4	A.5 Information security policies	5-Medium	7.91%
Goal 4-Inconsistency 2.48%	A.6 Organisation of information security	1-Minor/No importance	1.74%
	A.7 Human resource security	1-Minor/No importance	1.74%
	A.8 Asset management	3-Low	3.99%
	A.9 Access control	1-Minor/No importance	1.74%
	A.10 Cryptography	1-Minor/No importance	1.74%
	A.11 Physical and environmental security	1-Minor/No importance	1.74%
	A.12 Operations security	4-Low Medium	5.62%
	A.13 Communications security	4-Low Medium	5.62%
	A.14 System acquisition, Dev and maintenance	1-Minor/No importance	1.74%
	A.15 Supplier relationships	9-Very important	26.95%
	A.16 Information security incident management	7-Vey high	15.63%
	A.17 InfoSec aspects of BCM	7-Vey high	15.63%
	A.18 Compliance	5-Medium	8.18%
Goal 5	A.5 Information security policies	9-Very important	18.82%
Goal 5-Inconsistency 3.05%	A.6 Organisation of information security	6-High	7.17%
	A.7 Human resource security	8-Important	13.13%
	A.8 Asset management	2-Very Low	1.77%
	A.9 Access control	3-Low	2.60%
	A.10 Cryptography	1-Minor/No importance	1.23%
	A.11 Physical and environmental security	8-Important	13.82%
	A.12 Operations security	5-Medium	5.07%
	A.13 Communications security	5-Medium	5.07%
	A.14 System acquisition, Dev and maintenance	1-Minor/No importance	1.23%
	A.15 Supplier relationships	2-Very Low	1.77%
	A.16 Information security incident management	2-Very Low	1.77%
	A.17 InfoSec aspects of BCM	6-High	7.17%
	A.18 Compliance	9-Very important	19.36%
Goal 6	A.5 Information security policies	1-Minor/No importance	1.24%
Goal 6-Inconsistency 2.74%	A.6 Organisation of information security	1-Minor/No importance	1.24%
	A.7 Human resource security	1-Minor/No importance	1.24%
	A.8 Asset management	5-Medium	4.38%
	A.9 Access control	7-Vey high	8.74%
	A.10 Cryptography	5-Medium	4.38%
	A.11 Physical and environmental security	1-Minor/No importance	1.24%
	A.12 Operations security	8-Important	12.77%
	A.13 Communications security	8-Important	12.77%
	A.14 System acquisition, Dev and maintenance	8-Important	12.77%
	A.15 Supplier relationships	8-Important	12.77%
	A.16 Information security incident management	4-Low Medium	3.10%

A.4.2 Domain Mapping per Risk

Table 20. Domain Mapping Per Risk 1/3

Risks	Domains	Level of importance domain/risk	In %
Risk 1	A.5 Information security policies	5-Medium	8.47%
Risk level: High	A.6 Organisation of information security	1-Minor/No importance	2.04%
Risk 1-Inconsistency 1.35%	A.7 Human resource security	1-Minor/No importance	2.04%
	A.8 Asset management	1-Minor/No importance	2.04%
	A.9 Access control	1-Minor/No importance	2.04%
	A.10 Cryptography	6-High	11.72%
	A.11 Physical and environmental security	1-Minor/No importance	2.04%
	A.12 Operations security	7-Very high	16.27%
	A.13 Communications security	8-Important	22.49%
	A.14 System acquisition, Dev and maintenance	1-Minor/No importance	2.04%
	A.15 Supplier relationships	1-Minor/No importance	2.04%
	A.16 Information security incident management	7-Very high	16.27%
	A.17 InfoSec aspects of BCM	1-Minor/No importance	2.04%
	A.18 Compliance	5-Medium	8.47%
Risk 6	A.5 Information security policies	7-Very high	7.94%
Risk level: Medium	A.6 Organisation of information security	5-Medium	3.43%
Risk 6-Inconsistency 2.02%	A.7 Human resource security	5-Medium	3.43%
	A.8 Asset management	8-Important	12.49%
	A.9 Access control	7-Very high	7.94%
	A.10 Cryptography	4-Low Medium	2.27%
	A.11 Physical and environmental security	1-Minor/No importance	1.05%
	A.12 Operations security	8-Important	12.49%
	A.13 Communications security	8-Important	12.49%
	A.14 System acquisition, Dev and maintenance	9-Very important	18.78%
	A.15 Supplier relationships	4-Low Medium	2.27%
	A.16 Information security incident management	6-High	5.19%
	A.17 InfoSec aspects of BCM	4-Low Medium	2.27%
	A.18 Compliance	7-Very high	7.94%
Risk 8	A.5 Information security policies	6-High	6.51%
Risk level: Medium	A.6 Organisation of information security	2-Very Low	1.75%
Risk 8- Inconsistency 2.27%	A.7 Human resource security	1-Minor/No importance	1.26%
	A.8 Asset management	7-Very high	9.79%
	A.9 Access control	7-Very high	9.79%
	A.10 Cryptography	1-Minor/No importance	1.26%
	A.11 Physical and environmental security	1-Minor/No importance	1.26%
	A.12 Operations security	8-Important	15.14%
	A.13 Communications security	5-Medium	4.39%
	A.14 System acquisition, Dev and maintenance	8-Important	15.14%
	A.15 Supplier relationships	5-Medium	4.39%
	A.16 Information security incident management	7-Very high	9.79%
	A.17 InfoSec aspects of BCM	5-Medium	4.39%
	A.18 Compliance	8-Important	15.14%
Risk 10	A.5 Information security policies	4-Low Medium	7.22%
Risk level: Low	A.6 Organisation of information security	1-Minor/No importance	1.96%
Risk 10 - Inconsistency 1.82%	A.7 Human resource security	1-Minor/No importance	1.96%
	A.8 Asset management	6-High	13.44%
	A.9 Access control	6-High	13.44%
	A.10 Cryptography	1-Minor/No importance	1.96%
	A.11 Physical and environmental security	9-Very important	29.67%
	A.12 Operations security	2-Very Low	3.25%
	A.13 Communications security	2-Very Low	3.25%
	A.14 System acquisition, Dev and maintenance	1-Minor/No importance	1.96%
	A.15 Supplier relationships	1-Minor/No importance	1.96%
	A.16 Information security incident management	6-High	13.44%
	A.17 InfoSec aspects of BCM	2-Very Low	3.25%
	A.18 Compliance	2-Very Low	3.25%
Risk 13	A.5 Information security policies	4-Low Medium	3.80%
Risk level: High	A.6 Organisation of information security	8-Important	13.25%
Risk 13-Inconsistency 2.27%	A.7 Human resource security	4-Low Medium	4.58%
	A.8 Asset management	7-Very high	8.93%
	A.9 Access control	9-Very important	13.94%
	A.10 Cryptography	1-Minor/No importance	1.31%
	A.11 Physical and environmental security	1-Minor/No importance	1.31%
	A.12 Operations security	7-Very high	8.93%
	A.13 Communications security	8-Important	13.94%
	A.14 System acquisition, Dev and maintenance	9-Very important	18.19%

Table 21. Domain Mapping Per Risk 2/3

Risks	Domains	Level of importance domain/risk	%
Risk 14	A.5 Information security policies	8-Important	15.77%
Risk level: Low	A.6 Organisation of information security	8-Important	15.77%
Risk 14- Inconsistency 2.42%	A.7 Human resource security	5-Medium	4.30%
	A.8 Asset management	5-Medium	4.30%
	A.9 Access control	5-Medium	4.30%
	A.10 Cryptography	1-Minor/No importance	1.27%
	A.11 Physical and environmental security	1-Minor/No importance	1.27%
	A.12 Operations security	7-Very high	9.50%
	A.13 Communications security	7-Very high	9.50%
	A.14 System acquisition, Dev and maintenance	5-Medium	4.30%
	A.15 Supplier relationships	6-High	7.21%
	A.16 Information security incident management	3-Low	2.30%
	A.17 InfoSec aspects of BCM	4-Low Medium	3.70%
	A.18 Compliance	8-Important	15.77%
Risk 16	A.5 Information security policies	5-Medium	6.20%
Risk level: Medium	A.6 Organisation of information security	7-Very high	15.51%
Risk 16- Inconsistency 1.34%	A.7 Human resource security	1-Minor/No importance	1.54%
	A.8 Asset management	7-Very high	15.51%
	A.9 Access control	7-Very high	15.51%
	A.10 Cryptography	6-High	10.13%
	A.11 Physical and environmental security	1-Minor/No importance	1.54%
	A.12 Operations security	5-Medium	6.20%
	A.13 Communications security	5-Medium	6.20%
	A.14 System acquisition, Dev and maintenance	5-Medium	6.20%
	A.15 Supplier relationships	5-Medium	6.20%
	A.16 Information security incident management	5-Medium	6.20%
	A.17 InfoSec aspects of BCM	1-Minor/No importance	1.54%
	A.18 Compliance	1-Minor/No importance	1.54%
Risk 17	A.5 Information security policies	5-Medium	2.66%
Risk level: Medium	A.6 Organisation of information security	8-Important	10.00%
Risk 17 - Inconsistency 1.74%	A.7 Human resource security	1-Minor/No importance	0.98%
	A.8 Asset management	6-High	4.09%
	A.9 Access control	8-Important	10.00%
	A.10 Cryptography	9-Very important	15.87%
	A.11 Physical and environmental security	7-Very high	6.27%
	A.12 Operations security	8-Important	10.00%
	A.13 Communications security	8-Important	10.00%
	A.14 System acquisition, Dev and maintenance	7-Very high	6.27%
	A.15 Supplier relationships	5-Medium	2.66%
	A.16 Information security incident management	5-Medium	2.66%
	A.17 InfoSec aspects of BCM	5-Medium	2.66%
	A.18 Compliance	9-Very important	15.87%
Risk 18	A.5 Information security policies	7-Very high	9.13%
Risk level: Medium	A.6 Organisation of information security	5-Medium	3.66%
Goal 18-Inconsistency 1.55%	A.7 Human resource security	1-Minor/No importance	1.20%
	A.8 Asset management	1-Minor/No importance	1.20%
	A.9 Access control	7-Very high	9.13%
	A.10 Cryptography	6-High	5.27%
	A.11 Physical and environmental security	1-Minor/No importance	1.20%
	A.12 Operations security	7-Very high	9.13%
	A.13 Communications security	6-High	5.44%
	A.14 System acquisition, Dev and maintenance	9-Very important	21.09%
	A.15 Supplier relationships	7-Very high	9.86%
	A.16 Information security incident management	7-Very high	9.13%
	A.17 InfoSec aspects of BCM	6-High	5.44%
	A.18 Compliance	7-Very high	9.13%

Table 22. Domain Mapping Per Risk 3/3

Risks	**Domains**	**Level of importance domain/risk**	**%**
Risk 20	A.5 Information security policies	7-Very high	11.76%
Risk level: Low	A.6 Organisation of information security	6-High	8.19%
Risk 20-Inconsistency 2.52%	A.7 Human resource security	1-Minor/No importance	1.46%
	A.8 Asset management	6-High	8.19%
	A.9 Access control	1-Minor/No importance	1.46%
	A.10 Cryptography	5-Medium	5.74%
	A.11 Physical and environmental security	1-Minor/No importance	1.46%
	A.12 Operations security	8-Important	16.90%
	A.13 Communications security	8-Important	16.90%
	A.14 System acquisition, Dev and maintenance	1-Minor/No importance	1.46%
	A.15 Supplier relationships	1-Minor/No importance	1.46%
	A.16 Information security incident management	4-Low Medium	4.05%
	A.17 InfoSec aspects of BCM	4-Low Medium	4.05%
	A.18 Compliance	8-Important	16.90%
Risk 22	A.5 Information security policies	7-Very high	9.16%
Risk level: Medium	A.6 Organisation of information security	7-Very high	9.16%
Risk 22- Inconsistency 1.90%	A.7 Human resource security	8-Important	14.59%
	A.8 Asset management	7-Very high	9.16%
	A.9 Access control	1-Minor/No importance	1.29%
	A.10 Cryptography	5-Medium	4.19%
	A.11 Physical and environmental security	1-Minor/No importance	1.29%
	A.12 Operations security	8-Important	14.59%
	A.13 Communications security	8-Important	14.59%
	A.14 System acquisition, Dev and maintenance	1-Minor/No importance	1.29%
	A.15 Supplier relationships	1-Minor/No importance	1.29%
	A.16 Information security incident management	5-Medium	4.19%
	A.17 InfoSec aspects of BCM	7-Very high	9.16%
	A.18 Compliance	6-High	6.02%
Risk 23	A.5 Information security policies	7-Very high	7.83%
Risk level: High	A.6 Organisation of information security	5-Medium	3.63%
Risk 23- Inconsistency 2.41%	A.7 Human resource security	1-Minor/No importance	1.15%
	A.8 Asset management	8-Important	12.02%
	A.9 Access control	5-Medium	3.63%
	A.10 Cryptography	1-Minor/No importance	1.15%
	A.11 Physical and environmental security	1-Minor/No importance	1.15%
	A.12 Operations security	8-Important	12.02%
	A.13 Communications security	8-Important	12.02%
	A.14 System acquisition, Dev and maintenance	9-Very important	18.29%
	A.15 Supplier relationships	5-Medium	3.63%
	A.16 Information security incident management	5-Medium	3.63%
	A.17 InfoSec aspects of BCM	7-Very high	7.83%
	A.18 Compliance	8-Important	12.02%

A.4.3 Risk mapping per domain step 8

Tables 23 and 24 give risk mapping per domain and correspond with step 8 in Figure 3.

Table 23. Risk mapping per domains A5 - A11

ID	A.5 Information security policies	A.6 Organisation of information security	A.7 Human resource security	A.8 Asset management	A.9 Access control	A.10 Cryptography	A.11 Physical and environmental security
Risk 1	5-Medium	1-Minor/No importance	1-Minor/No importance	1-Minor/No importance	1-Minor/No importance	6-High	1-Minor/No importance
Risk 6	7-Very high	5-Medium	5-Medium	8-Important	7-Very high	4-Low Medium	1-Minor/No importance
Risk 8	6-High	2-Very Low	1-Minor/No importance	7-Very high	7-Very high	1-Minor/No importance	1-Minor/No importance
Risk 10	4-Low Medium	1-Minor/No importance	1-Minor/No importance	6-High	6-High	1-Minor/No importance	9-Very important
Risk 13	8-Important	8-Important	8-Important	8-Important	9-Very important	1-Minor/No importance	1-Minor/No importance
Risk 14	8-Important	8-Important	5-Medium	5-Medium	5-Medium	1-Minor/No importance	1-Minor/No importance
Risk 16	5-Medium	7-Very high	1-Minor/No importance	7-Very high	7-Very high	6-High	1-Minor/No importance
Risk 17	5-Medium	8-Important	1-Minor/No importance	6-High	8-Important	9-Very important	7-Very high
Risk 18	7-Very high	5-Medium	1-Minor/No importance	1-Minor/No importance	7-Very high	6-High	1-Minor/No importance
Risk 20	7-Very high	6-High	1-Minor/No importance	6-High	1-Minor/No importance	5-Medium	1-Minor/No importance
Risk 22	7-Very high	7-Very high	8-Important	7-Very high	1-Minor/No importance	5-Medium	1-Minor/No importance
Risk 23	7-Very high	5-Medium	1-Minor/No importance	8-Important	5-Medium	1-Minor/No importance	1-Minor/No importance

Table 24. Risk mapping per domains A.12-A.18

ID	A.12 Operations security	A.13 Communications security	A.14 System acquisition, Dev and maintenance	A.15 Supplier relationships	A.16 Information security incident management	A.17 InfoSec aspects of BCM	A.18 Compliance
Risk 1	7-Very high	8-Important	1-Minor/No importance	1-Minor/No importance	7-Very high	1-Minor/No importance	5-Medium
Risk 6	8-Important	8-Important	9-Very important	4-Low Medium	6-High	4-Low Medium	7-Very high
Risk 8	8-Important	5-Medium	8-Important	5-Medium	7-Very high	5-Medium	8-Important
Risk 10	2-Very Low	2-Very Low	1-Minor/No importance	1-Minor/No importance	6-High	2-Very Low	2-Very Low
Risk 13	7-Very high	8-Important	7-Very high	1-Minor/No importance	5-Medium	1-Minor/No importance	8-Important
Risk 14	7-Very high	7-Very high	5-Medium	6-High	3-Low	1-Minor/No importance	1-Minor/No importance
Risk 16	5-Medium	5-Medium	5-Medium	5-Medium	5-Medium	1-Minor/No importance	1-Minor/No importance
Risk 17	8-Important	8-Important	7-Very high	5-Medium	5-Medium	5-Medium	9-Very important
Risk 18	7-Very high	6-High	9-Very important	7-Very high	7-Very high	6-High	7-Very high
Risk 20	8-Important	8-Important	1-Minor/No importance	1-Minor/No importance	4-Low Medium	4-Low Medium	8-Important
Risk 22	8-Important	8-Important	1-Minor/No importance	1-Minor/No importance	5-Medium	7-Very high	6-High
Risk 23	8-Important	8-Important	9-Very important	5-Medium	5-Medium	7-Very high	8-Important