UNIVERSIDADE TÉCNICA DE LISBOA

INSTITUTO SUPERIOR DE ECONOMIA E GESTÃO

MESTRADO EM: Gestão de Sistemas de Informação

INFORMATION SYSTEMS SECURITY OUTSOURCING KEY ISSUES: A SERVICE PROVIDERS' PERSPECTIVE

LUÍS FILIPE XAVIER PEREIRA

Orientação: Doutor Mário Caldeira (ISEG-UTL)
Doutor Filipe de Sá-Soares (Universidade do Minho)

Júri:

Presidente: Engenheira Ana Lucas (ISEG - UTL)

Vogais: Mestre Winnie Ng Picoto (ISEG - UTL)
Doutor Mário Caldeira (ISEG - UTL)
Doutor Filipe de Sá-Soares (Universidade do Minho)

Abril 2011

LIST OF ACRONYMS

Acronym	Definition
IS	Information Systems
IT	Information Technology
SLA	Service Level Agreement

ABSTRACT

There is a perception that information systems security outsourcing, in spite entailing a relationship between a client and one or more providers, tends to be studied and analysed from the perspective of the client. A gap is then believed to exist in the study of the information systems security outsourcing relationship from the point of view of the service provider. This research aims to identify the key issues of such a relationship from the perspective of the service provider and rank them according to their importance. The Delphi method was used to support the communication with the group of experts contributing to this research as well as to boost consensus within the group. Final interviews with participants were also conducted with the aim of reaching deeper into their opinions and to shed a brighter light over the results of the Delphi. A ranked list of the 13 most important key issues found is presented and discussed and propositions for further work are put forward in the wake of the study.

Key words: information systems security, information systems security outsourcing, Delphi method, key issues study.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGMENTS

First and foremost, I would like to thank Rita Leal, my girlfriend, for all the support and motivation she gave me all along the way. It is impossible to ask for a better friend and companion.

Secondly, I would like to thank my parents, Conceição Xavier and Carlos Pereira, without whom this work would surely never come to life.

Lastly, I would like to thank Professor Mário Caldeira, but especially Professor Filipe de Sá-Soares for his unwavering guidance and support.

Thank you to all who contributed to the success of this study.

1 INTRODUCTION

Outsourcing constitutes partnerships that are instantiated in the form of contracts between at least two entities, namely the organization that intends to outsource and those organizations (service providers) that will perform the activities outsourced. A gap is believed to exist in research in what refers to the analysis of key aspects these partnerships should fulfil in the case of Information Systems (IS) security outsourcing, from the perspective of service providers, so that the relationship is successful.

This research aims to identify those key issues from the perspective of the service providers and rank them according to their perceived importance to a group of experts working for service providers in IS security.

It is believed that this research is of particular importance due to the delicate nature of its subject (the outsourcing of IS security activities by organizations) but also in deepening the understanding of the IS security outsourcing relationship so organizations can steer their path in the right direction.

The research question that will be addressed can be formulated in the following way: which are the key issues towards a successful IS security outsourcing relationship from the perspective of service providers?

In pursuing its objectives, this dissertation starts with a literature review, unveiling what academia has thought and published on the subject of IS security outsourcing and where it stands in IS outsourcing at large.

The methodological approach taken is then depicted, focusing strongly on what the Delphi method is and how it can be used in issues ranking studies. The design of the

study is also detailed as is the description of every Delphi round of the study and the final interviews.

Lastly, a comprehensive analysis of the findings of the study is presented and conclusions are drawn.

2 LITERATURE REVIEW

The following literature review focuses on what has academia published of relevance to the study at hand, which is to say, in the domain of IS security outsourcing and where this stands in IS outsourcing at large.

2.1 The Definition of Outsourcing

The most simple and brief definition of outsourcing is the buying of goods or services that used to be produced in-house. In the IS context and according to Kern and Willcocks (2001, p. 1) the outsourcing of IS will be "the handing over to a third party of the management and operation of an organization's IT assets and activities", as a whole or partially.

2.2 Issues Influencing the IS Outsourcing Decision

Ketler and Willems (1999) state that the outsourcing decision influencing factors can have origins such as economical, human resources, risk versus control, vendor and contract issues and lastly, strategic advantage. Each of these factors will be discussed briefly in the following subsections.

2.2.1 Economical

One of the reasons of resorting to outsourcing is the cost savings the buyer can materialize due to the economies of scale allowed to the vendors of services and products. This is one of the most common reasons in adopting outsourcing.
Economies of scale aside, knowing how vendors materialize cost savings also enables client managers to achieve them themselves.
The *hidden* costs of outsourcing have also to be considered. It is common to have outsourcing costs bigger than expected (Ketler and Willems 1999), whether through the underestimation of costs by the vendor or through an honest misinterpretation of the contract. In fact it is extremely difficult to predict years ahead the future evolution of IS use, nonetheless, it tends to happen in outsourcing contracts (Ketler and Willems 1999).

2.2.2 Human Resources

Outsourcing is a viable solution to two common problems in the human resources domain. First comes the difficulty in justifying the existence of full time technical specialists, and then comes the temporary peaks of demand of resources to develop systems. As the use of IS progresses and expands, it is nearly impossible for a small firm to have specialists in every domain. Outsourcing firms are capable of offering a wide range of skills and technical knowledge. Although outsourcing enables the client to access a wide pool of resources it might also weaken the IS function in terms of its competencies and know how.

2.2.3 Risk versus Control

Some IS managers envisage the decision of outsourcing as a risk versus control issue. Outsourcing will enable the transfer and sharing of risk with the service provider regarding the choice of technology and resource allocation, for example. But outsourcing also presupposes losing total control over, for example, IS quality, security and disaster recovery.

2.2.4 Vendor and Contract Issues

The difference between a successful outsourcing and a disaster may lie in the choice of service provider and in the terms of the contract. Analysing service providers should include their previous experience, their long term planning, their technology and human resources, their financial situation, and their work relationships and cultural adaptation. Contractual terms may consider service, duration and flexibility issues.
A good contract establishes performance measures and uses incentives and penalties regarding that performance.

2.2.5 Strategic Advantage

Even though the majority of organizations turning to outsourcing do so for tactical reasons, there is also a trend of doing it for strategic reasons. The intention is to use IS to improve critical aspects of the business. For example, Dow Chemical, an American organization of the chemical sector, noticed it was losing many elements of its IS team with unique business know how. It resorted to outsourcing and to one service provider in particular so as to provide new career perspectives to its collaborators as well as having access to a broader pool of talent. Another example is the Swiss National Bank

(the Swiss central bank) that bought a part of its outsourcing service provider with the intention of being able to sell IS outsourcing services to other financial services organizations (Ketler and Willems 1999).

2.3 The Outsourcing Relationship

The outsourcing relationship and what makes it work are the cornerstone of this thesis, therefore it is relevant to dwell on what the scientific community has researched on this topic, which is done in the subsections that ensue.

2.3.1 Outsourcing Relationship Types

In the IS domain, Nam et al. (1996) have found four outsourcing relationship types:

1. The Support type: this is the most traditional outsourcing relationship. Here service providers are typically not close to the IS core activities and contract duration is usually shorter. Within the range of activities there are contract programming, hardware maintenance, minor technical services and hardware or software installation. It is relatively easy to find alternative service providers.
2. The Reliance type: this type of relationship corresponds to the most popular outsourcing type during the 1990's. The famous IBM-Kodak outsourcing contract corresponds to this type of relationship. The IS functions targeted by this type of outsourcing are mostly non-core activities and cost reduction is one of the big motivations of resorting to this type of outsourcing. Contract duration is bigger than in the Support case because this type of relationship needs a higher degree of commitment between parties.

3. The Alignment type: IS consulting services or technical supervision of the planning and design of IS are examples of this type of relationship. Although here service providers are not close to operations, their impact lasts longer than in the Support type. The main difference lies in the fact that in the Alignment type, service providers are involved in more strategic IS functions.
4. The Alliance type: service providers substitute not only internal operations but are also responsible for strategic activities. Conception and planning of the design of a new product or system that helps reach a new market is an example of this kind of relationship. This type of outsourcing has the longest contract duration and the relationship requires a high level of commitment from both parties.

2.3.2 Outsourcing Relationship Key Issues

Several authors have discussed the qualities outsourcing relationship should embody to be successful.

Table 2-1 condenses what several authors have written on this topic.

Table 2-1 – Key issues or qualities in a successful outsourcing relationship.

Authors	Key issues / Qualities
Grover, Cheon, and Teng (1996)	Trust, Communication, Satisfaction, Cooperation
Kern (1997)	Communication
Nguyen, Babar and Verner (2006)	Trust
Lee and Kim (1999)	Trust, Commitment, Business Understanding, Sharing Benefits and Risks, Conflict

Authors	Key issues / Qualities
Goles and Chin (2005)	Trust, Commitment, Consensus, Flexibility (client perspective), Interdependence (service provider perspective)

From the analysis of Table 2-1, it can easily be concluded that trust is the most pervasive quality among all qualities identified by those researchers. It is faced as the one issue that should be present in an outsourcing relationship for it to blossom. According to Nguyen et al. (2006), trust enables a more open communication, an improved performance, better quality deliverables and a more satisfactory decision making process.

Communication is also an important issue, in fact, to Kern (1997) it is the single most important issue since it is through it that problems can be identified and alleviated.

Commitment is another relevant quality.

These identified qualities are influenced by a number of prior activities or conditions. These are illustrated in Table 2-2.

Table 2-2 – Prior conditions to a successful outsourcing relationship.

Authors	Conditions / Activities
Nguyen et al. (2006)	Credibility, Technical and managerial capacity, Performance in a pilot-project, Investment, Cultural understanding
Lee and Kim (1999)	Participation, Quality of Communication, Sharing of Information, Age of the relationship, Mutual dependency, Top Management Support

The two sets of authors do not overlap in the prior conditions they state. *A priori* they all seem relevant in promoting a successful outsourcing relationship.

2.3.3 Managing the Outsourcing Relationship

Immediately after its inception, the outsourcing relationship has to be managed and steered in the right direction.

The management tool will be, almost by definition, the outsourcing contract, but a too aggressive and literal reading of it may be counterproductive to the outsourcing relationship. Litigating should be a last resort and motivating should always be the way to a good relationship.

Table 2-3 illustrates what several authors have written on the topic of managing an outsourcing relationship.

Table 2-3 – Issues on how should an outsourcing relationship be managed.

Authors	What is relevant in managing the outsourcing relationship?
Nguyen et al. (2006)	Communication strategies, Conformity to the contract, Cultural understanding, Service provider capacity, Quality of the deliverables, Delivery on time, Commitment to improving processes, Expectation management, Personal relationships, Performance results
Lee and Kim (1999)	Active participation in a cooperative relationship, Sharing information to create a synergy that no company can achieve by itself, Build a trust-based relationship so that no partner behaves opportunistically

Authors	What is relevant in managing the outsourcing relationship?
McFarlan and Nolan (1995)	CIO function, Performance measures, Task coordination, Client-service provider interface
Lee et al. (2003)	Understand each other's business, Set short and long term goals, Clearly define realistic expectations, Share benefits and risks, Develop performance standards, Expect the existence of change and revision, Prepare for the unexpected, Nurture the relationship

It is important to stress the following concepts derived from Table 2-3: communication, understanding, commitment, expectation, participation, trust, coordination, sharing and nurturing. They all come into play when forging a sound outsourcing relationship.

2.4 The Definition of IS Security Outsourcing

IS security outsourcing is, according to Fenn, Shooter and Allan (2002), the transfer of an existing in-house IS security function to a third-party provider, as a whole or partially.

2.5 The Decision of Outsourcing IS Security

Rowe (2007), in relation to outsourcing costs and benefits, references Coase (1937), who discussed the costs associated with the market – the cost of pricing goods, the cost of learning about available goods, of learning about prices, negotiating contracts and

monitoring contractual performance, for example – and he predicted that outsourcing would expand as these costs decreased.

Modern society is built around specialization and more tasks are outsourced today than ever before (Schneier 2002). However, deciding to outsource IS security is difficult because the stakes are high so it is no surprise that paralysis is a common reaction when contemplating this decision (Shneier 2002).

Whether or not a company should outsource its IS security activities depends upon the company's unique organization, industry, geographic locations, management environment, legal, regulatory and contractual requirements and more. Organizations with minimal stores of sensitive information and who do not regard IT (Information Technology) as a core component of their business are more likely to outsource security than those who have significant volumes of sensitive information or consider IS part of their competitive advantage (Power and Forte 2005).

The decision to outsource has been discussed by several authors. Table 2-4 summarizes their views on this subject.

Table 2-4 – What should an IS security outsourcing decision be based on.

Authors	The outsourcing decision is based on…
Schneier (2002)	• Functions to outsource being complex, important or distasteful • Chief argument to outsource is financial
Power and Forte (2005)	• The risk outsourcing poses to the business • The ability of the business to provide such functions internally

Authors	The outsourcing decision is based on…
	• How much risk the business is willing to take in a responsible manner
Endorf (2004)	• Saving money • Having outside providers performing non-core competencies

To Schneier (2002) functions that are outsourced have one of three characteristics: complexity, importance, or distastefulness. He considers IS security to have all three. To him the chief argument to outsource IS security is financial. A company can get expertise much cheaper through outsourcing. Outsourcing companies can spread costs and knowledge across all customers.

Endorf (2004) has a similar take: outsourcing can be used as a successful tool for saving an organization's money while allowing outside providers to perform non-core competencies.

The outsourcing decision is, at the end of the day, a trade-off between acceptable risk and acceptable cost of security (Fenn et al. 2002).

2.6 The Market for IS Security Outsourcing

Networks have become increasingly complex as the need to enable customers, partners and employees access to one's network increases. The threat of security breaches and problems seems to be increasing at a rapid rate. The cost of breaches and virus attacks can reach into the billions of US dollars. According to Endorf (2004) it is estimated that the worldwide impact of malicious code was USD $13.2 billion in 2001 alone. Data loss

and hacking attempts could easily cost a company more, in addition to other negative effects such as loss of reputation.

The "Information Security Survey 2001" by Ernst & Young stated that only 19% of respondents had outsourced IS security (Fenn et al. 2002). Power and Forte (2005) defend that the collapse of the technology bubble in 2001 hurt the trend but it is picking up.

In 2003, Gartner predicted that for the Western European market, the managed security services would be the fastest growing service type across all vertical markets in the period 2002-2006. Gartner expected outsourced security monitoring and management market to grow at a combined annual rate of 31% through 2005 (Tsohou et al. 2007).

Endorf (2004) states that KPMG surveyed 641 senior managers to do a study in 2002 and 66% of organizations were outsourcing security to some extent.

According to the CSI/FBI surveys of 2005 and 2006 (Tsohou et al. 2007), 37% and 39% of respondents, respectively, outsource. In addition, 10% in 2005 and 12 % in 2006 outsource more than 20% of the security function. Larger companies seem to outsource a higher percentage of their IS security function. The CSI computer crime and security survey of 2009 states that respondents reported a notable reduction in the amount of security functions outsourced. In 2009, 71% of respondents stated that they do not outsource any security functions at all while the year before only 59% of respondents made that statement.

Rowe (2007) described the study by RTI between 2004 and 2005 aimed at understanding firms' IS security investment decisions. This study included 36 organizations that contributed data and 21 other that, though not providing data, agreed

to discuss the issues. The organizations represented a variety of sectors and the relevant results are displayed in Table 2-5.

Table 2-5 – Percentage of companies that outsource, by industry (Rowe 2007).

Company Type	Installation, Implementation and Maintenance	Monitoring of IT Security Issues	Vulnerable Assessment/ Planned Compromise	Purchase Third-Party Insurance	Purchase Legal Consultation (Internal or External)
Financial	50.0%	50.0%	100.0%	50.0%	83.3%
Healthcare	66.7%	0.0%	33.3%	33.3%	66.7%
Manufacturing	83.3%	33.3%	66.7%	0.0%	50.0%
Other	40.0%	20.0%	80.0%	40.0%	60.0%
Small Business	66.7%	66.7%	66.7%	16.7%	66.7%
University	14.3%	0.0%	14.3%	0.0%	57.1%
Average	52.8%	27.8%	58.3%	22.2%	63.9%

According to the study, firms spend approximately 5.7% of their IT budgets on IT security. The 2006 CSI/FBI study found it to be approximately 5.0% of IT spending. In 2009, the "Information Security Survey" (Ernst & Young 2009) conveyed that outsourcing of security functions was the activity in which the greatest number of respondents (18%) said they planned to reduce their spending on and in which the least amount of participants (14%) stated they would spend more in 2010. It revealed a definite unwillingness of many organizations to outsource their security functions. The majority of respondents indicated that they had no plans to outsource most of their security-specific activities.

2.7 IS Security Outsourcer's Required Features

Endorf (2004) argues that it is generally better to deal with a firm with which a relationship already exists and provides a general procedure to help identify a good service provider:

- Research providers among current vendors one is doing business with;
- Confirm that providers have the experience sought;
- Other aspects worth considering are:
    - The breadth of services. Is security their main focus?
    - Financial stability;
    - Does the company contribute to the information security community as a whole by publishing articles, for example?
    - Does it offer 24/7 support?
    - How many employees does it have?
    - Does it have a strong response time?
    - Does it use the best-of-breed technologies?
    - Is it referenced by other customers?
    - What are its limitations in terms of what it can and cannot do?
- Make sure there is a definite understanding of what is asked of the provider. Put the proper SLAs (Service Level Agreements) in place together with the legal contracts.

Power and Forte (2005) focus on assuring the outsourcer has a well trained staff in the functions they would be performing and that it can independently assess the professional qualifications of their security-related personnel. It should also have clearly articulated procedures and policies for handling a wide range of scenarios and their operation should satisfy a wide spectrum of security standards applicable to its target markets.

Schneier (2002) advises on avoiding situations of conflict of interest by service providers (e.g., sell and manage security products).

2.8 Advantages and Disadvantages of IS Security Outsourcing

The benefits of outsourcing IS security are intimately linked to the benefits of outsourcing IS. Fenn et al. (2002) list a set of benefits that can be achieved through outsourcing IS security:

1. IS security is a specialist competency that many believe is best left to experts. This allows a company to focus on its core competencies.
2. The standard of outsourced IS security is normally higher than the in-house equivalent. External outsource providers are typically high skilled individuals up-to-date with the latest security loop-holes and appropriate patches. Tough SLAs have to be met by the provider. The in-house service provider is not under the same pressure to deliver.
3. A company carrying out its own IS security will need to deal with numerous suppliers and a multitude of contracts. Outsourcing will replace that with only one commercial relationship while placing the customer in a stronger negotiating position.
4. There are potential cost savings: faster learning curve, economies of scale, and more efficient processes.

Endorf (2004) extends the previous list of advantages assuming both the decision to outsource and the decision not to outsource. These can be seen in Table 2-6 together with the disadvantages he identifies in both situations.

Table 2-6 – Advantages and disadvantages of outsourcing IS security (Endorf 2004).

Decision	Advantages	Disadvantages
Not to outsource	Knowledge and talent remain in-house with professionals who understand the organization's core business	The financial impact of staffing and retaining security professionals can be substantial
	Employee security professionals can keep the company's best interest in hand because it directly reflects on their job security	An employee being internal does not guarantee that he can be trusted more than an external one
	Turnover among outsourcing staff is usually at a much higher rate than with internal employees	Employee staffing is less flexible
	Management control is much better when employees are used	_
To outsource	There will be the expertise needed 24/7, 365 days a year	External associates will have access to the organization's information
	The company will not have the financial impact of hiring or training several full-time security professionals	Outsourcing can cause friction with internal employees because the perception can be that internal employees are more loyal to the organization
	There will be SLAs in place	There can be cultural challenges between the way the outsourced company does things and the organization's internal processes
	Service providers have a broader industry	_

Decision	Advantages	Disadvantages
	view because they can more easily see what other organizations are experiencing	
	Staffing flexibility is available because it is much easier to change an external staff member than an internal employee	
	Extra capacity in unforeseen events is available	

Since it is impossible to identify and track every weakness of the systems, risk can never be eliminated, only managed and contained and therefore Fenn et al. (2002) state several disadvantages of outsourcing IS security:

1. The service provider has its own operational risks;
2. Outsourcing security might cause breaches of confidentiality; and
3. The start of an outsourcing relationship will require some upfront cost.

However, when organizations outsource some security activities, positive network externalities may accrue to other firms who outsource security activities to the same firm. This happens because if the latter provides services to different companies, when a problem is solved in one of them, the rest will have the solution at hand when they face the same problem.

Rowe (2007) states that outsourcing IS security can solve the problem of the sharing of information about security breaches and potential solutions. Through outsourcing IS security to one firm, it would have more data to perform analysis on and would therefore provide better solutions to clients but it would also be a single point of failure.

Still according to Rowe (2007), two additional risks are involved in IS outsourcing: stealing proprietary information (copy customer information and selling it to competitors) and post-contractual renegotiation (an opportunistic repricing after the outsourcer feels locked-in).

2.9 The IS Security Outsourcing Relationship

According to Tsohou et al. (2007) organizational culture influences the way IS security is perceived, the way security countermeasures are adopted and the way the organization reacts to the cultural changes of a new security program. In IS security management outsourcing, cultural differences may arise between the countermeasures applied by the provider and the company's internal policies.

Still according to the same authors, the ISO/IEC 17799:2005 standard identifies the consistency between the IS security management systems and the organizational culture as a critical success factor.

Outsourcing success does not depend only on contractual aspects but also on the relationship between clients and vendors. Examining this relationship is then critical.

Six factors have been identified to affect the IS security outsourcing outcome. Table 2-7 illustrates them and how they can be managed according to Tsohou et al. (2007).

Table 2-7 – How to manage the IS security outsourcing relationship (Tsohou et al. 2007).

Factor	How to manage it?
Participation	Exploring the different underlying assumptions about security related

Factor	How to manage it?
	concepts through a process of security communications
Communication quality	Exploring the underlying assumptions of the two organizational security cultures
Mutual understanding	Seeking ways to redefine and loosen the group boundaries of the members of both organizations
Information sharing	Providing information about internal business objectives and processes and enforcing security knowledge sharing
Top management support	Top management should timely and clearly define the roles, responsibilities and authorities that the employees of both organizations will undertake
Coordination	It is a prerequisite for all other factors

According to Fenn et al. (2002) service levels are important but can be difficult to define. Unlike other areas of outsourcing, there are no blueprints.

Table 2-8 illustrates what questions should be settled in the outsourcing contract.

Table 2-8 – Questions that should be settled in the outsourcing contract (Fenn et al. 2002).

The outsourcing contract should…
Specify the detailed provision for downtimes and availability of systems
Lead to service credits whenever there are fails in meeting service levels
Allow for the client to terminate the contract if the service levels are constantly missed
Include a 'key personnel' clause preventing the best team negotiated during the pitch phase of the deal from being replaced with a "B team"
Consider innovative thinking and decision-making that are embedded in IS security, therefore arising

The outsourcing contract should…
intellectual property rights questions
Address data protection regarding personal data ensuring its confidentiality, integrity and availability
State what will be done by both parties when the client thinks the service provider has breached security

It is in the service provider interest to impose stringent service levels because this is nurturing its best asset: reputation.

To Endorf (2004) managing IS security outsourcing includes following best practices, conducting due diligence, defining the requirements and defining roles and responsibilities.

Alner (2001) states that great attention must be given to determining which parts of the IS security function should be performed by the outsourcing company and which should be handled by the client. The client company should reserve some of its staff to monitor the security work handled by the outsourcer, but Alner (2001) remembers that SLAs are a two-way street and both parties have to fulfill their part of the agreement.

Fenn et al. (2002) argue that outsourcing IS security is only as effective as the relationship between the outsource provider and customer. So finding the right provider and agreeing appropriate and workable service levels are of paramount importance.

2.10 Conclusion

The outsourcing of IS security is a somewhat unexplored field in IS literature. The rare occurrences of articles dealing with this topic tend to assume the client's perspective leaving the service provider's perspective as almost uncharted territory.

Schneier (2002), Fenn et al. (2002), Endorf (2004), Rowe (2007) and Power and Forte (2005), which is to say the majority of articles found dealing with the topic of IS security outsourcing, take the point of view of the client looking to find whether outsourcing IS security is the way to go and providing a roadmap to do so.

This asymmetry may stem from the also asymmetrical relationship outsourcing tends to be, typically pinned in favor of the client.

Since outsourcing implies a relationship, which automatically presupposes the existence of two or more parties, and since the point of view of the service provider has somewhat been neglected in academic literature, it makes sense to pursue the research objectives set for this dissertation work.

3 METHODOLOGICAL APPROACH

The present study relied methodologically on the Delphi method and on the Q-sort technique. Both are explained in the following sections.

Interviews were also conducted after the final Delphi round.

3.1 Introduction to the Delphi Method

To Linstone and Turoff (1975) the Delphi method can be characterised as a structured group communication process that is efficient in allowing individuals to deal with a complex problem. To achieve this structured communication a measure of feedback is given to participants regarding their own answers and regarding the answer of the group as a whole. It gives participants the possibility of correcting or revising their answers and it provides a degree of anonymity towards the individual answers of each participant.

The Delphi method is an iterative consensus method in which a group of experts in a specific domain are inquired individually and anonymously about issues pertaining to their domain of expertise. Although a multitude of different ideas may arise, it is expected that the feedback given to participants regarding the answer of the group as a whole will forge a consensus opinion.

3.1.1 Origin and Application of the Delphi Method

The Delphi method was born out of a series of studies conducted at the RAND Corporation in the 1950's (Williams and Webb 1994). It was used mainly in technological foresight.

The reasons that originally justified the use of the Delphi method were several: precise information not being available or difficult or expensive to obtain; evaluation models require subjective information as input to the point that it becomes the dominant parameter of the model. When these circumstances arise, the use of the Delphi method should be considered (Linstone and Turoff 1975).

There are still other circumstances where the use of the Delphi method can be considered such as when the study dwells upon decisions or judgments that allow group involvement or when a group decision process may boost the outcome of the study and reinforce its findings (Hasson, Keeney, and McKenna 2000).

Turoff (1970) identified four research goals that may justify the use of the Delphi method:

- Explore or expose information or underlying assumptions that induce different judgments;
- Search for information that might generate consensus within a group;
- Correlate informed decisions regarding a topic that spans a multitude of subjects; and
- Educate the answering group as to the diversity of angles of a topic and its interrelationships.

In taking the decision of using the Delphi method, one of the following properties of a study might indicate that its use should be considered (Linstone and Turoff 1975):

- The problem at hand cannot be solved by analytical techniques but can benefit from subjective collective judgments;
- The individuals from whom a contribution to the analysis of a complex problem is expected have diverse backgrounds in what comes to experience and competence;
- More individuals are needed than those that can effectively interact face to face;
- Time and cost do not allow frequent face to face meetings;
- Severe misunderstandings or completely differing points of view between participants may lead to the implementation of a communication process such as the one in the Delphi method; and
- The heterogeneity of the participants must be preserved, avoiding domination by quantity or strength of character.

General examples of the application of the Delphi method are building the structure of a model, outlining the pros and cons of potential political options and the development of causal relationships between economic and social phenomena.

The Delphi method has been a somewhat popular tool in IS research. Some examples of its application are the following:

- Several key issues studies in IS management were conducted using the Delphi method. These studies aimed at unveiling which issues in IS management were most poignant to IS executives and how did they all relate in terms of importance. Two of these studies were performed by Brancheau, Janz, and Wetherbe in 1987 and 1996;
- A study performed by Holsapple and Joshi (2002) identifying and characterizing knowledge manipulation activities within knowledge management episodes and

developing a framework for knowledge flows was conducted using the Delphi method;

- Organizational mechanisms for enhancing user innovation in IT were studied by Nambisan, Agarwal, and Tanniru (1999) in which they used the Delphi method to support their conceptual propositions; and
- In an international study conducted by Schmidt et al. (2001) for identifying software project risks, a ranking-type Delphi was used to produce a rank-order list of risk factors.

3.1.2 Dynamics of the Delphi Method

This section explores the dynamics of the Delphi method, focusing on the conditions prior to its inception and discussing the procedures that have to be undertaken while conducting a study.

There is no set of universal guidelines for conducting a Delphi study but it is important to be careful when introducing changes to the structure that is most commonly used in Delphi studies.

As remarked by Linstone and Turoff (1975, p. 5) “In its design and use Delphi is more of an art than a science”.

The Delphi method is an iterative multistage process designed to combine opinions into group consensus (McKenna 1994). Experts are asked to answer, in the various rounds of the process, to questionnaires developed and sent by the research team. The questionnaires are answered individually by participants, who typically know the research team but not the other experts contributing to the study. In each subsequent round, the new questionnaire will be enriched with the consolidated results of the

previous round as well as with the answer to the last round provided by the particular expert to whom the new questionnaire is now being sent to. A statistical analysis of the round data will lead to an understanding of where the collective opinion lies and when it is shared with participants in the next round, it will enhance the motion towards consensus because experts will be able to tune their answers.

The iterative process will go on until an acceptable level of consensus is reached or the research team decides to halt the study because no observable motion towards consensus was observed.

Whenever possible, a pilot-test should be performed with a reduced set of experts before the implementation of the study.

3.1.2.1 Important Aspects to Consider in the Initial Design of the Study

An important aspect, which can affect the perception of validity and trust on a study, is the level of consensus at which it is assumed that the group has achieved consensus and no longer makes sense to perform another round of questionnaires.

If the level of consensus set is not reached round after round, prolonging rounds without any appreciable movement in the direction of greater consensus will tax experts (Schmidt 1997), possibly leading to diminishing returns round after round. However, the rate of no-response tends to be low in the Delphi method due to the assurance (sometimes verbal assurance) by each expert to the researcher that they will participate in the study (Okoli and Pawlowski 2004). It is, nonetheless, important to keep experts actively involved in the process until it is completely halted. The decision regarding the level of consensus is extremely important but there is no unique and universally accepted answer to it.

This question is intertwined with the stopping criteria of the study and has to be tackled from three different angles.

The first is determining how many rounds will be necessary to reach the predetermined consensus level. The answer depends on the definition of consensus, on how much time there is available, on the nature of the study itself (having one or several research questions), and on the fatigue of the group of participants (Hasson et al. 2000). Literature shows that the classical Delphi study involved four rounds, but nowadays two or three rounds seem to be preferred (Hasson et al. 2000).

Knowing when to stop the study is paramount. If halted too early, its outcome might not be satisfactory. If halted too late it might tax the group of participants and possibly lead to the dropout of several of them, endangering the study and sliming the possibility of it meeting its objectives.

The second angle is the level of consensus set *a priori* as the threshold level after which the panel of participants is considered to be in agreement. This level will depend on factors such as the size of the answering group, the objective of the research and time and resources available. A statistical parameter by which agreement in a certain round can be measured is Kendall's coefficient of concordance (Schmidt 1997) or Kendall's *W*. Using *W*, one can make a realistic determination of whether consensus has been reached, whether consensus is increasing and the relative strength of consensus. To help interpreting the result of the calculation of Kendall's *W*, Table 3-1 is provided.

Table 3-1 – Interpretation of Kendall's coefficient of concordance (Schmidt 1997).

W	Interpretation	Confidence in Ranks
0.1	Very weak agreement	None
0.3	Weak agreement	Low
0.5	Moderate agreement	Fair
0.7	Strong agreement	High
0.9	Unusually strong agreement	Very high

Agreement between two different rounds can be calculated using a statistical parameter like Spearman's rank-order correlation coefficient (*rho*), which emphasizes the magnitude of difference between ranks (Schmidt 1997). After this calculation, if the result is that the two different rounds are strongly correlated, then stopping the rounds should be considered since there is no appreciable change in the answer of the group. The third and final angle is the number of items that are carried over from one round to the next. Reducing the number of items being ranked can promote consensus. Too many of them can just be clouding the group consensus (Schmidt 1997).

Studies employing the Delphi method use what McKenna (1994) defines as a panel of informed individuals. Before the selection process starts, a definition of expert to the study should be put forward. This is sensitive and must be managed carefully because a bad selection process can lead to biased conclusions.

Regarding the representativeness of the sample, the broader it is the greater its potential for the best ideas to come up. Studies have shown that heterogeneous groups are more creative than homogeneous ones (Okoli and Pawlowski 2004). On the other hand, the subject being researched can be so complex that only a small number of experts exist, limiting the size of the Delphi group.

It should be highlightet that the number of participants of the Delphi group is not dependent or guided by *statistical strength* to gain significance in the way a standard inquiry-based study would. The Delphi method depends mostly on the group dynamics in order to reach consensus. Literature recommends between 10 and 18 participants as the normal requirement to conduct a successful Delphi study (Okoli and Pawlowski 2004).

In the Delphi method, experts are selected to apply their knowledge to a certain problem on the basis of criteria, developed from the nature of the problem being researched (Hasson et al. 2000). When participants are not selected randomly, the representativeness of the sample is not assured in a statistical sense. This criteria-based selection of the Delphi method relies on the assumption that researchers have what it takes to pinpoint who should be part of the group of participants.

When starting a Delphi study, experts can be invited *a priori* (although this is not mandatory) to participate in the forthcoming study and in numbers that render the study possible and valid.

Experts have their own motivations to participate in such studies. It can be being chosen for a diversified but selective group, having the opportunity to learn from the process of strengthening consensus, and the increased visibility within its organization or externally to it (Okoli and Pawlowski 2004).

Managing communication with the group of participants is very important. Right from the invitation, participants need to be informed of what they will be asked to do, of how much time they will spend and how the information they contribute will be used (Hasson et al. 2000).

Traditionally, the administration of Delphi surveys was paper based. Increasingly, however, the use of electronic communications is employed, requiring participants to be computer literate (Hasson et al. 2000). Using electronic media such as email and the World Wide Web presents several advantages when compared to traditional paper and pencil and direct mail. Important to the Delphi method is how they speed up the turnaround time between questionnaires (Okoli and Pawlowski 2004), while being also less expensive. Regarding the quality of answers, several studies refer that web-based questionnaires are better especially when open questions are used (Santos and Amaral 2004).

Another advantage of electronic media is that, when using the Q-sort technique (described in 3.2.1) together with Delphi, a web-based tool will make sure its procedure is strictly followed by participants.

The disadvantage in using general web-based questionnaires is their low response rate (Santos and Amaral 2004).

3.1.2.2 The Course of the Delphi Study

To Linstone and Turoff (1975), the typical Delphi undergoes four different phases:

i. Exploring the subject under discussion wherein each individual contributes with the additional information he feels pertinent to the issue;
ii. Reaching an understanding of how the group views the issue;
iii. Exploring disagreements within the group and the reasons for those disagreements; and

iv. A final evaluation when all information has been gathered and analysed and evaluations have been fed back for consideration.

The process of collecting opinions starts with the first round, which in the classical Delphi consists of a set of open-ended questions. They are open with the intention of not hindering the generation of ideas, and allowing the maximum degree of freedom in the answers. This will help identify the issues that will be dealt with in subsequent rounds. Participants are encouraged to contribute with as large a volume of opinions as they can. Schmidt (1997) recommends that at least six ideas be asked of each participant. Different participants will probably come up with the same issues but phrasing them differently. The researcher will have to consolidate a list in which the ideas and opinions are not overlapping. In some studies, the topics will be gathered beforehand and the Delphi starts by asking experts to rank them in order of importance. It must be recognized that this approach could bias the responses (Hasson et al. 2000). On the other hand this last approach saves time by not requiring one initial round to collect items and could still preserve creativity if participants are allowed to add items they think are relevant.

Regarding data analysis the Delphi has a qualitative and a quantitative nature. If the first round is an open round where participants are asked to provide a certain number of ideas as raw material for the rest of the Delphi, then an effort has to be done to group similar items. This is the qualitative nature of the Delphi. Close attention must be paid to this activity since there is the possibility of misinterpreting opinions placing them in opinion groups foreign to their true meaning, with the overall list short of a relevant item. The expressions used by participants in their own opinions should be preserved, as

far as possible, when transposing them to the consolidated items. Whitman in 1990 and Green et al. (1999), as remarked by Hasson et al. (2000), mention that those opinions that are less frequent may be omitted rendering the list of consolidated opinions easier to manage. This, however, will go against the basic tenets of the Delphi method. Participants themselves should judge items in terms of quality, not researchers (Hasson et al. 2000).

In rounds after the first, it will also be important to supply summaries to participants regarding the statistical analysis performed on data from the previous round. Central tendency measures like the average and dispersion levels like the standard deviation should be considered. This will allow participants to frame their own opinion on what is conveyed as the *group opinion*. To report findings a number of different approaches have been used, including graphical presentation and textual presentation of statistical results encompassing central tendency measures, standard deviation and rankings.

The presented results should be capable of showing the evolution throughout the rounds of both the results themselves and the degree of participation by experts.

Follow-up interviews will enable the collection of additional relevant data and a deeper understanding of the research questions.

3.1.3 Advantages of the Delphi Method

Being able to decide in situations where the available information is incomplete or contradictory has boosted the use of *consensus methods*, among which, the Delphi method. Studies have consistently shown that for questions requiring expert judgment, the average of individual responses is inferior to the averages produced by group decision processes (Okoli and Pawlowski 2004).

The Delphi method relies on the safety of numbers, which is to say, several people will be less prone to error than just one. As no completely right answer exists, the consensus of a group of experts will be the next best thing.

The Delphi method collects the various opinions without the necessity for the participants to physically meet. A meeting might even be impossible to arrange if experts live in geographically diverse places.

The method also allows for opinions to be given in a non-competitive way, providing a degree of freedom and individuality to participants towards their own opinions and expressions.

The anonymity provided by the Delphi method is one of its most distinctive characteristics and sets it apart from other consensus methods. Although they are most of the times anonymous to each other, participants are not anonymous to the researcher. This allows the latter to perform follow-up activities for further clarification.

The controlled interaction between the various participants seems to be the process that best leads to independent thought by all participants. Direct confrontation all too often induces the hasty formulation of preconceived notions, an inclination to close one's mind to novel ideas, a tendency to defend a stand once taken or a predisposition to be swayed by persuasively stated opinions of others (Dalkey and Helmer 1963).

3.1.4 Disadvantages of the Delphi Method

Careful thought must be given to using the Delphi method. There are key issues surrounding problem identification, researcher skills and data presentation that must be addressed (Hasson et al. 2000).

Due to its flexibility, literature reports studies with modified forms of the Delphi that have been criticized for lacking methodological rigor (Hasson et al. 2000). This can jeopardize the study and its conclusions. It is therefore important to clearly define upfront all decisions regarding the methodological approach adopted.

Using feedback to participants to build consensus can also be a bias generator. Ultimately, achieving a certain consensus does not mean the right opinion, idea, or judgment was found.

Additionally, any research strategy implies doubts regarding validity.

Threats to the validity of the Delphi method stem mostly from pressures for convergence of predictions which undermine its forecasting abilities (Hasson et al. 2000). Content validity can be enriched by participants and validity itself can be strengthened by challenging all assumptions round after round.

One other important factor affecting validity is the response rate (Hasson et al. 2000). If there is an insufficient response rate the outcome can more easily be biased.

Among the common reasons for the Delphi method to fail the following stand out:

- The researcher imposes a preconceived notion on the participants (through over specifying the study), not allowing other perspectives to stand out;
- Assuming that the Delphi might be a substitute for all other human communications in a given situation;
- Using insufficient presentation and summarization techniques on the group answer;
- Ignoring and not exploring disagreements in such a way that those that are in disagreement exit the study, generating an artificial consensus; and

- Underestimating the demanding nature of the Delphi method (Linstone and Turoff 1975).

Apart from these relevant criticisms, the Delphi method is also the target of *virtual* criticisms. Virtual insomuch as not being believed to affect the utility of the method:

- Selecting a good respondent group: this problem is common to the formation of any group activity – panels, committees, study groups, etc.
- Every time a design of a Delphi specific to a certain application is assumed to represent all Delphis. Here the problem is coming up with a too explicit and restrictive definition of what a Delphi is;
- Questioning the honesty of the research team, which is something common to any research team, irrespective of the chosen method; and
- Differences of logic and language level when participants come from different cultural backgrounds (Linstone and Turoff 1975).

3.1.5 Final Considerations on the Delphi Method

The success of a Delphi study depends on the researcher performing operational tasks successfully such as keeping in touch with participants throughout the various rounds and analysing their changes of opinion.

The Delphi method is a versatile tool that researchers might use at different stages of their investigation. The use of this method for foresight as well as identification and prioritization of issues can be valuable for example in the selection of topics and definition of research questions. It might also be helpful in identifying variables of interest or in formulating propositions.

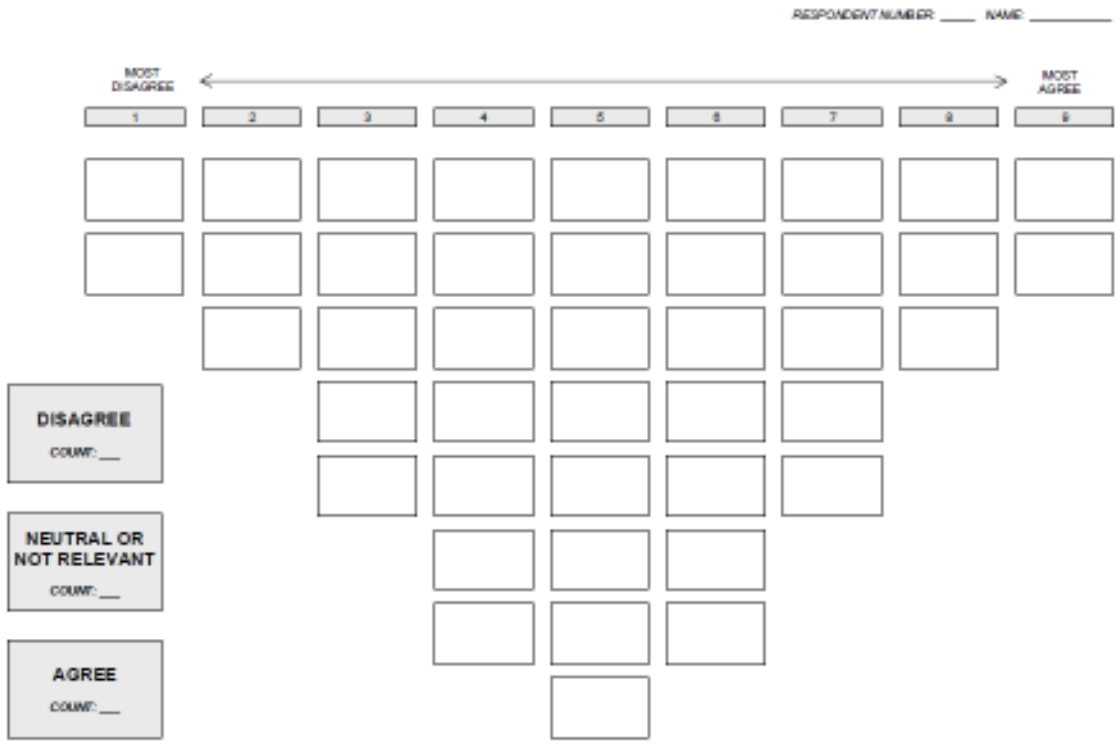
3.2 Introduction to the Q Technique

The Q technique supplies a foundation for the systematic study of subjectivity inherent to a person's point of view (Brown 1993).

3.2.1 Q-sorting

In a Q study people are presented a sample of statements (Q-set), numbered randomly, about a certain topic. The group of respondents (P-set) is then asked to rank-order the statements from its own point of view using a *quasi-normal* distribution. It is also handed out a score sheet and a distribution that participants should use in the ranking process. The score sheet will be a continuum of integer values between two extremes such as *least agreement* and *most agreement* and between these extreme values a distribution resembling the normal takes form.

An example of a score sheet and distribution is provided in Figure 3-1.



Source: van Exel and de Graaf (2005, p.30)

Figure 3-1 – Score sheet for Q-sort.

Researchers start by asking participants to read all statements carefully and to divide them in three sets: one grouping the statements with which they agree, one with the statements with which they disagree and one with statements they feel neutral about. The number of statements in each group is registered to check for agreement-disagreement balance in the Q-set. The participants are then asked to fill the provided score sheet. Conducting follow-up interviews with respondents is recommended so they can elaborate on their points of view, especially on the reasons that made them place statements on the edges of the score sheet.

3.2.2 Delphi Method and Q-Sort Technique

Using the Delphi method together with the Q-sort technique instead of, for example, a Likert scale (the most common option when using the Delphi with ranking purposes) happens because one of the objectives of the study is to rank items according to their importance. Likert scales have the inconvenient that the respondent only considers one item at a time, individually, and not as part of a whole. By considering items independently it becomes difficult to ponder on their relative importance according to the scale, tending towards extreme values. This results in a high probability of repetitions in the ranking of items which goes against the goal of the study which is to provide a list of their relative importance (Santos and Amaral 2004).

Using the Q-sort technique that problem is solved because the participant will have to look at all the items as a whole, divide them into three groups (the most important, the least important and the neutral ones) and rank them according to a predetermined *quasi-normal* distribution. Therefore a rank-ordered list of items is produced without ambiguities and with a slim probability of having repetitions (Santos and Amaral 2004).

3.3 Designing the Study

The goal of this study, as previously stated, was to uncover the key issues regarding outsourcing relationships in the IS security domain, from the point of view of service providers. The study is geographically limited to Portugal.

Methodologically, it was decided to rely on the Delphi method and the Q-sort technique as the research tools capable of allowing the study to reach its goals. The combination of Delphi method with Q-sort technique was selected for several reasons, namely:

- The study dwells upon decisions or judgments that allow group involvement or a group decision process may boost the outcome of the study and reinforce its findings;
- The problem at hand cannot be solved by analytical techniques but can benefit from subjective collective judgments;
- Time and cost do not allow frequent face to face meetings;
- The Delphi method has been applied successfully to studies with similar objectives such as the key issues studies performed by Brancheau, Janz and Wetherbe (1987, 1996);
- Using Q-sort together with Delphi helps participants to consider all items as a whole when ranking them and not just one at a time, which improves the ranking part of the study.

The use of the Delphi method will then comprise the following tasks to be completed before the rounds cycle can start:

1. Selection and invitation of experts;
2. Definition of the communication process with experts;
3. Deciding on open or closed rounds;
4. Operationalization of the Delphi method with Q-sort; and
5. Definition of stopping criteria.

Each of these steps will be detailed in the subsections that follow.

These tasks were performed in the months leading up to March 2010, when the rounds cycle started.

3.3.1 Selection and Invitation of Experts

The process of selecting and inviting experts to the study is of the utmost importance because their ideas and opinions will determine the richness and quality of the outcome of the study. Besides providing the raw matter to the study, it is the controlled interaction between experts that will enable the study to meet its goals. It is also a sensitive subject because it can generate bias.

The process of selection and invitation of experts started with building a list of companies operating in Portugal and advertising IS security services through their corporate website or were known to provide these services. The list is presented in Table 3-2:

Table 3-2 – Companies operating in Portugal that provide IS security services.

GMS Consulting	Prológica	Novabase
Accenture	IBM	Capgemini
Everis	Microsoft	Deloitte
PriceWaterhouseCoopers	KPMG	PT-SI
Sinfic	Panda Security	Glintt
Tecnidata	Mainroad	CSO – Chief Security Officers
Unisys	Symantec	Compta

The first approach in trying to reach someone at manager or senior consultant level in those companies and working in the IS security field was to use the researcher's own network of acquaintances and ask them for someone with the desired background and current position within their organization (encompassing the companies listed). This approach led to seven experts, who were invited to participate in the study and from whom the researcher got an agreement of participation. They represent the following

companies: Capgemini, IBM, Prológica, GMS Consulting, everis and KPMG (two experts belong to the same company). Leads for Accenture and PT-SI were followed but with no practical results. All contacts with potential participants were done through email and the invitation typically contained the following items:

1. Convey the main subject of the study;
2. Convey the nature of the study, the need to invite experts and mention that the person fits the profile sought;
3. Explicit invitation to participate;
4. Explicit reference to the identity and organization of the supervising professors and their contacts; and
5. Guarantee the complete confidentiality of the contribution to the study, guarantee complete anonymity and guarantee that no question regarding the internal processes of their organizations would be asked.

According to Okoli and Pawlowski (2004), a group between 10 and 18 experts is acceptable to conduct a Delphi study. The number of experts agreeing to contribute to the study had not yet reached this target, meaning the invitation and selection process had to continue.

The second approach was to draw from Table 3-2 the list of companies where no expert had yet been contacted and search their corporate website for a way to contact the company directly, asking for the message to be relayed to someone with the characteristics sought and mentioning the invitation items above. Six companies were contacted this way (PriceWaterhouseCoopers, CSO, Compta, Delloite, Microsoft, and Sinfic), yielding no experts to the panel of participants since no feedback was obtained.

A third and final approach was undertaken in trying to reach a number of participants that enabled the Delphi to produce more robust results. This approach relied on using the Linkedin professional social network to browse for people with the characteristics that were pursuit *vis-à-vis* their background and current position. Linkedin has a functionality that shows through which people is a person connected to another pertaining to one's network (contacts to the third degree). Since the ultimate goal will be to contact experts through the people that bind us, searches within Linkedin were restricted by one's own network of contacts to the third degree. Seven invitations were sent, leading to seven experts who all agreed to participate. The companies they represent are: Novabase, Unisys, Glintt, Mainroad, PT-Prime, Symantec, and Panda Security.

A panel of 14 participants was considered enough to conduct a successful Delphi.

Table 3-3 – Companies the participants work for.

GMS Consulting	Prológica	Novabase
Everis	IBM	Capgemini
Unisys	KPMG	PT-SI
Panda Security	Mainroad	Glintt
	Symantec	

3.3.2 Definition of the Communication Process with Experts

After the experts agreed to participate in the study the communication process entailed with participants followed a few rules:

1. An email initiated each round conveying information about:
    a. The objective of the round;

   b. The time period it would be open to answers;
   c. The link and credentials that would enable the participant to answer the round;
   d. A guarantee of confidentiality and anonymity;
   e. Highlight of the importance of their contribution to the outcome of the study;
   f. Disclosure of the researcher's contacts for any unforeseen circumstance;
   g. In rounds after the second one, conveying a brief description of the consensus obtained in the previous round;
2. A reminder was sent to participants two days before the answering period ended (if it was a week day and if the participant had not yet responded) and on the day the answering period ended;
3. One extension to the answering period was allowed, never exceeding one week;
4. If there were any contacts made by participants an answer by the researcher was mandatory.

This study required participants to have access to an email (and to the Internet). As remarked by Okoli and Pawlowski (2004), normally, this might be a serious biasing factor, however, for a study employing experts in IS security, this is not an unreasonable requirement.

It should also be highlighted that all interactions with participants were in Portuguese as was the formulation of the key issues.

3.3.3 Deciding on Open or Closed Rounds

The researcher decided to perform a blank sheet first round. This means that the first round of the Delphi process will be used to collect from participants their opinions on what are the key issues surrounding a successful IS security outsourcing relationship. This was a necessity since no relevant issues were identified in literature specifically for the case of IS security outsourcing and focusing on the point of view of the service provider.

It was also decided to conduct open rounds (in which participants can add new items they think are relevant) until a round comes in which no items are added.

3.3.4 Configuring the Web Tool Supporting the Delphi with Q-sort

A web tool was used to administer questionnaires to participants in the various rounds of the study and help them abide the rules of the Delphi with Q-sort, which in the Q-sort part can be complex to participants not familiar with the technique. It also served as a repository of answers from which data could be retrieved to be analysed by the researcher.

The decision of using a web tool was mostly based on the fact that it speeds up the turnaround time between questionnaires and that is an important factor in the Delphi process. It is also expected that the answer rate will not be lower just because a web tool is being used since the panel is small and the researcher has had prior confirmation of participation by all experts involved.

Part of the authentication screen of the web tool is presented in Figure 3-2.

Figure 3-2 – Authentication screen of the e-Delphi web tool

For a user with configuration privileges the tool has the following screens, each with its own functionalities:

- The ‘Studies’ screen where the records of studies lay, where it is possible to create new studies, to finish or edit them and where it is possible to navigate to the rounds of a study;
- The ‘Rounds’ screen where the records of rounds lay, where it is possible to edit a round, check its results and the details of the answers by participants;
- The ‘Issues/Experts’ screen where it is possible to check the issues of the round and also navigate to the answers of participants;
- The ‘Answer’ screens, one with a simple rank of the answers of participants and another one with the Q-sort answer of respondents ; and
- The ‘Round Results’ screen where the round results are summed up.

The configuration needed to conduct a Delphi initially consists of creating the study, giving it a name and a brief description, choosing the type of the study (whether it uses Q-sort or not and whether it uses a first round blank sheet or not), loading the research

question, registering participants data and defining their authentication credentials, and setting a date for its start and end.

Typical configuration of rounds consists of setting its start and end date and also, if it is a ranking round, on setting which issues will be ranked on that round.

3.3.5 Definition of Stopping Criteria

Before the start of a Delphi study, the criteria for stopping it should be clearly stated. The interaction between the experts' opinions will lead to a varying level of consensus. This level can be calculated but there is a need to determine at which level is considered that experts have reached consensus. Achieving utter consensus is a utopia and pursuing it would be costly in terms of time while rendering no extra results.

Prolonging rounds indefinitely would certainly trigger the *law* of diminishing returns if experts were to be taxed with too large a number of rounds of questionnaires.

On the other hand, stopping the study too early could hinder its outcome as well, possibly because no valuable results were attained.

For this study, the set of stopping criteria has three rules:

1. Kendall's *W* of the round should be equal or greater than 0.7;
2. Spearman's *rho* between rounds should be equal or greater than 0.9; and
3. If the criteria above are not met when the fourth round is reached then the study will stop at the end of the fourth round.

The first rule deals with the consensus between participants in a given round. As stated in subsection 3.1.2.1 the statistical parameter by which agreement in a certain round will be measured is the Kendall's coefficient of concordance or Kendall's *W*. According to

Table 3-1 a value of 0.7 is considered to be the lowest threshold for a strong agreement between participants.

The second rule deals with the stability of answers between consecutive rounds. As stated in subsection 3.1.2.1 Spearman's *rho* measures the magnitude of difference between ranks. A Spearman's *rho* equal to 0.9 will confirm that no appreciable change happened between these consecutive rounds and the study should be halted because the collective answer stabilized.

The third rule establishes a maximum number of rounds to achieve consensus. As stated in subsection 3.1.2.1 the classical Delphi typically implies four rounds.

These criteria will not be applied to the first round since it is a round aimed at collecting issues.

4 DESCRIPTION OF THE STUDY

The Delphi study involved the administration of four rounds of questionnaires and a final interview to the participants of the fourth round.

The analysis of each round and final interviews is detailed in the following sections.

4.1 Delphi Rounds

4.1.1 First Round

The first round was a blank sheet round, which is to say, a round in which participants were asked to provide, following the suggestion of Schmidt (1997), at least six issues that, from their point of view, are key in the success of an IS security outsourcing relationship from the service provider standpoint. These issues were collected by the researcher as the raw material that, after a consolidation process, would result in the issues to be presented to participants and which they should ponder and rank.

The alternative to having a blank sheet first round would be to collect the relevant issues from literature and then presenting them to experts but still allowing them to add new issues to the list. This alternative was set aside because searching the relevant literature did not provide a list of the issues deemed relevant for the subject of the study from the service providers' perspective. This means the current study is treading new ground. This being the case, a blank sheet first round is in fact the best option. The participants, being familiar with the topic at hand, would produce themselves the factors that they would rank later on in the study.

The first round started on March 19th and ended on March 26th. An extension period of four days was given to participants to ensure a higher answering rate. At the end of the round 10 experts had answered it and four were unable to do so.

Fifty seven issues were provided by participants. These raw issues underwent a process of consolidation. This process consisted of grouping similar items beneath an umbrella issue encompassing all similar items, and formulating a statement to denominate the group of issues and a statement to provide a brief description aimed at clarifying the overall issue. After a few iterations this process was considered complete and a list with 25 consolidated issues was its outcome. Table A-1 in Annex A presents all 25 issues. The order in which they are numbered is random and does not reflect any kind of ranking.

4.1.2 Second Round

In the second round participants were asked to rank the list of 25 consolidated issues from the first round according to their own point of view. The ranking of issues resorted to the Q-Sort technique which is embedded in the web tool that mediated the administration of questionnaires. The items were presented to participants in a list where their position was completely random.

The second round took place between April 19th and April 26th. An extension period of four days was again allowed to participants so that the answering rate could be higher. At the end of the round 10 experts had answered it and four were unable to do so.

The detailed and ranked list of issues resultant of the second round is presented in Table A-2 of Annex A.

When two or more issues obtained the same ranking, the one with lower standard deviation came first in the overall ranking.

The data collected by the Delphi questionnaire on this round was analysed from two different angles. The first was to juxtapose the answers provided by the participants in this round with the issues that each one of them provided in the first round. The aim was to get a glimpse of whether the participants would pick *their* issues from the consolidated and vote them favourably or would otherwise favour issues from other participants. In fact, the mix of these two reasons makes it impossible to get a notion of whether they see themselves in the consolidated list of issues. If participants, after looking at the list of consolidated issues, think that one or more important issues are missing, they had the opportunity and possibility in the second round of adding it to the list for future rounds. None did so and this can be perceived as the participants seeing *their* issues in the consolidated list, thus validating it. The situations in which an issue from an expert had a low score from that same expert are attributed to the fact that other issues, which that individual participant had not thought about, were considered more important when it came to scoring them.

The second angle of analysis was the consensus achieved by all answers to the second round and for that Kendall's W was calculated.

The value calculated for Kendall's W is

$$\text{Kendall's } W = 0.231 \ (p < .001)$$

According to Schmidt (1997) this reveals a weak agreement among experts.

None of the stopping criteria were met and so a third round ensued.

4.1.3 Third Round

Before starting the third round of the Delphi questionnaire two decisions had to be taken. The first dealt with continuing to allow participants to add new issues to the list. Since no participant added new issues to the list in the second round, it was decided to no longer allow that possibility to participants and thus the list was considered closed to new issues. The second decision was about reducing the set of issues to be ranked by participants in this third round. The decision was to trim the five issues that were considered less important in the second round. This decision was taken to circumvent two problems: on one hand, the third round was going to ask of experts that they, once again, rank the list of issues according to their own point of view and doing it on a list of 20 issues would reduce their cognitive effort and possibly motivate them to continue answering the questionnaire. On the other hand, with 20 factors in comparison to 25, consensus was expected to rise. The promotion of consensus is essential since the objective of the study is to not only provide a list of the most relevant issues in the IS security outsourcing relationship from the point of view of the service provider but to present these issues in a ranking that is a consensus ranking within a group of experts. To reach this goal, the promotion of consensus is not only correct but also advised.
The third round took place between May 14th and May 20th. For the third straight time, an extension period of four days was allowed to participants so that the answering rate could be higher. The items were presented to participants in the order of importance given by the group as a whole in the previous round, from most important to least important. At the end of the round, nine experts had answered it and five were unable to do so.

The detailed and ranked list of issues resultant of the third round is presented in Table A-3 of Annex A.

The outcome of the round was measured in terms of consensus and in terms of convergence between this round and the previous one. Respectively, the Kendall's *W* was calculated together with the Spearman's *rho*.

Kendall's $W = 0.120$ ($p = .361$)

Spearman's *rho* $= 0.614$ ($p = .004$)

This value of Kendall's *W*, according to Schmidt (1997), shows a weak agreement among participants and is in fact worse in terms of consensus than the Kendall's *W* calculated in the previous round. Confidence in ranks is quite low, bordering none. Regarding Spearman's *rho*, it shows that although the answer to these two rounds can be correlated positively, a movement occurred between rounds and so it is possible to conclude that the experts' collective answer did not stay static to a degree that it would be better to stop the study.

None of the stopping criteria were met and so a fourth and last round must ensue.

4.1.4 Fourth Round

Before starting the fourth round a decision had to be taken regarding the reduction of the list of issues to be considered by participants in this round. The first intention was to trim 10 issues to the list. Consensus in the third round was weak and since the fourth is the last round it was considered a good trade-off to reduce the list of issues to 10 and boosting the possibilities of consensus by having a shorter list. Deeper analysis of the 10 issues coming last in the third round classification enabled taking a better decision regarding how many issues to trim. Relying only on the relative position of the issues in

the ranking to decide on what issues to trim can be misleading because the confidence in ranks is quite low and the active panel was composed of only 10 experts. Bringing to the analysis the mode and how many participants scored that issue in the first 10 positions, as shown in Table 4-1, is relevant.

Table 4-1 – Third round's last 10 issues analysis.

Rank: 3rd Round	Mode	<= 10 (% of experts)
11	5	56%
12	6/11	33%
13	10	67%
14	14	33%
15	4/5/11/12/13/14/15/18/20	22%
16	15/16	22%
17	18	22%
18	7/16/17	33%
19	19	33%
20	20	33%

Taking in consideration the results shown in Table 4-1 it is possible to conclude that regarding the mode the top three issues should not be trimmed. Regarding the percentage of experts that scored the issue in the first 10 positions, the 11th and 13th issues belong together with the first 10. Taking into consideration this new information it was decided to trim the last seven issues so the fourth round will present to participants 13 issues to rank.

The fourth round took place between June 11th and June 17th. Again an extension period of four days was allowed to participants to improve the answering rate. All 13 items were presented to participants ranked according to the importance given to them in the

previous round by the group as a whole. Fourteen experts were asked to participate in the fourth and final round of the study. Nine experts conveyed their point of view while five were unable to do so.

The detailed and ranked list of issues resultant of the fourth round is presented in Table A-4 of Annex A.

Once again the Kendall's *W* was calculated together with the Spearman's *rho*.

Kendall's $W = 0.120$ ($p = .374$)

Spearman's *rho* $= 0.324$ ($p = .280$)

Again Kendall's *W* shows weak agreement among participants and is still worse in terms of consensus than the Kendall's *W* calculated in the second round. Confidence in ranks is low. Regarding Spearman's *rho*, it shows that the third and fourth rounds can be correlated positively but not to a degree that it could be stated that no change occurred in the experts' answers.

The third of the stopping criteria was met and consequently the questionnaires were halted.

Using descriptive statistics, the fourth round was further analysed with the aim of understanding the dispersion of choice for each particular issue among the various participants. The results are presented in Table 4-2.

Table 4-2 – Descriptive statistics of the participants' answer to the fourth round.

	4th Round Answers								
Issue Denomination	**Maximum**	**Minimum**	**Range**	**First Quartile**	**Median**	**Third Quartile**	**Interquartile Range**	**Lower Limit for Moderate Outliers**	**Upper Limit for Moderate Outliers**
Clear definition of responsibilities of the client and of the IS security services provider	12	2	10	4	9	11	7	-6,5	21,5

	4th Round Answers								
Issue Denomination	**Maximum**	**Minimum**	**Range**	**First Quartile**	**Median**	**Third Quartile**	**Interquartile Range**	**Lower Limit for Moderate Outliers**	**Upper Limit for Moderate Outliers**
Credibility of the IS security services provider	9	1	8	3	6	8	5	-4,5	15,5
Safeguard of the client's information confidentiality by the IS security service provider	11	1	10	6	6	10	4	0	16
Quality of services delivered by the IS security provider	13	2	11	4	6	8	4	-2	14
Existing trust in the relationship between client and IS security services provider	12	1	12	1	2	7	6	-8	16
Experience of the IS security provider in providing such services	13	4	9	7	10	13	6	-2	22
Cost-benefit ratio of the IS security service from the client's point of view	11	1	10	5	7	8	3	0,5	12,5
Capability to evaluate the level of the IS security service performed	11	5	6	5	5	9	4	-1	15
Response time of the IS security service provider	12	3	9	5	6	8	3	0,5	12,5
Evidence of the capability of the IS security services provider to perform the service in question	13	1	12	1	7	13	12	-17	31
Human resources competencies of the IS security services provider	12	2	10	5	7	10	5	-2,5	17,5
Existence of a business continuity plan	13	3	10	4	9	12	8	-8	24
Existence of successful previous relationships between the client and the service provider	13	3	10	4	10	11	7	-6,5	21,5

The average interquartile range is ~5.7 which confirms the significant dispersion of choice among participants for a set of only 13 items.

The existence of outliers would only be possible in two items ("Cost-benefit ratio of the IS security service from the client's point of view" and "Response time of the IS security service provider") as can be inferred by the upper limit column for moderate outliers. Due to the value in question, the existence of a moderate outlier would still be extremely improbable.

4.1.5 Analysis of the Delphi Rounds

The Delphi study relied on the input of 14 experts. Their participation throughout the rounds is depicted in Table 4-3.

Table 4-3 – Participation of experts throughout the rounds.

Participant	Round 1	Round 2	Round 3	Round 4
P1	✔	✘	✘	✔
P2	✘	✘	✘	✘
P3	✔	✔	✔	✔
P4	✘	✔	✘	✘
P5	✔	✔	✔	✔
P6	✔	✔	✔	✔
P7	✔	✔	✔	✔
P8	✘	✔	✔	✔
P9	✔	✔	✔	✔
P10	✔	✔	✔	✔
P11	✔	✘	✘	✘
P12	✔	✘	✘	✘
P13	✘	✔	✔	✘
P14	✔	✔	✔	✔

All participants' answers to the ranking rounds (second, third and fourth) are shown in Annex C, and in each plot it is possible to compare the individual answers to the group answer. The plots account only for the ranking rounds and the group answer is shifted one position to the right to help understand the influence that is exerted on the participants' answers to the next round.

Apart from participant P2, who never conveyed his opinion in any of the rounds and from participants P11 and P12, who only participated in the initial round where items were collected from participant's opinions, all other participants contributed with their opinion in one or more ranking rounds. For these, an individual analysis of answers ensues.

Participant P1 gave his opinion only in the fourth round. It is largely coincident with the group's answer. One factor remained in strong disagreement, curiously it was the item that the group deemed most important.

Participant P3's answers seem to be headed in the direction of the group's answers since in six factors the participant's answer goes in the direction the group in the previous round. For the other seven items the direction coincides in one round but not in both. A slight volatility is noticed namely in the credibility issue.

Participant P4 only participated in the second round and thus was not influenced by the opinion of the group. His opinion seems to diverge from the group's answer.

The answers given by participant P5 are quite volatile through the rounds. Only the item related to the competencies of human resources seems somewhat steady. The participant does not seem moved by the group answer and no significant convergence effort is seen. Only in four items the participant follows the tendency outlined by the group.

Participant P6 also shows a degree of volatility in his answers and does not seem to be persuaded by the group's answer.

Participant P7 shows a volatility that seems linked to the convergence effort in aligning with the group's answers.

Much like P7, P8 seems to have adjusted his answers to the opinion of the group. This is even more the case for the fourth and final round.

The convergence effort is also noticed for participant P9, although in this case it seems more significant for the third round.

Participant P10 shows the biggest convergence effort of all participants. In spite of this, for two items the tendency is completely divergent to the group's opinion.

Participant P13 is the one making the least effort to align with the group. For five factors his answers are going in the complete opposite direction compared to the group. This might be explained by the fact that he answered to two ranking rounds, which is to say one ranking round knowing the group's answer. This may have limited his convergence effort *vis-à-vis* other participants that answered the three ranking rounds.

Participant P14 shows the same tendency as P13 but in a milder manner.

Considering the experts that answered to all ranking rounds, there were 104 items that were classified as shown in Annex C. This classification dealt with the convergence effort done by participants. Of these 104 only 41 convey a consistent effort by participants to align with the group's answers. This means that the convergence effort as a whole is not significant throughout the study.

Volatility is an issue for several of the participants. This could be explained by the convergence effort of each participant, trying to move towards the group's answer. Since the convergence effort was deemed not significant, other reasons have to come into play. A possible explanation would be the fact that participants do not have strong opinions and if they are not aware of their previous answers when they rank items then a significant shift might be observed.

Regarding an overall similar answering behavior by experts, there is a mild trend, which could be explained by the fact that, round after round, the number of items is being reduced which inevitably leads to putting the given items (ultimately 13) in the first

positions. Another mild trend noticed is the match of participants' answers to the groups', but when the latter changes an overshoot effect seems to arise on the part of the participants.

4.2 Interviews

After three ranking rounds, consensus among participants was still weak even after reducing the set of items to rank from 25 to the 13 most important.

The analysis had to reach deeper into the motivations and reasons of the participants to answer like they did, which meant that an extra effort had to be made in order to interview the experts.

Interviews were proposed to the participants of the fourth and last round, and six of them (P5 to P10) accepted the invitation and had the opportunity to convey their opinions through a telephone interview that took on average 15 minutes and was recorded with the consent of the interviewees. The interview script was simple and involved discussing the motivations of the participants to having selected the top three items they did in the fourth round, prompted by the question "Why are they the most important?". Then the group's top three items were conveyed and the possible match or mismatch of opinions was discussed. In analysing the interviews, the recordings were replayed and every independent aspect mentioned by each interviewee was highlighted. All aspects were then compared and consolidated leading to several remarks.

From a general point of view, when addressing their top three items and the reasons for their choice, participants assumed two perspectives. The more common was seeing the client and the relationship as a future client and a future relationship, which still have to

be won. The success factors of the relationship are taken for the items that enable the selling of the service (cost-benefit ratio, credibility, and experience). This perspective contrasted with the one that focused on the factors that enabled a good ongoing relationship (response time, definition of responsibilities, and the existence of a business continuity plan) and the possibility of assessing the service being provided.

Most participants focused on the price of the service as a key point to winning the client and also maintaining the service and the relationship. Items such as quality of service, experience of the service provider and existence of previous successful relationships take second place behind this important factor. The price factor takes precedence when the service being delivered is not differentiated and is seen as a commodity to a large extent. The client does not understand the real value of the service and sometimes decision-makers are not aware of the value of certain services. For the clients that understand the value of IS security, their demand tends to be based on the quality of the service and not as much on the price.

According to some participants, the motivation for some clients to outsource is the reduction of their costs. This however cannot be done successfully if the client does not know itself and does not know its processes. Knowing itself is a critical success factor if the outsourcing service and relationship is to be successful. The maturity level of organizations also has to be high enough for them to resort to outsourcing successfully. According to one participant the existence of a business continuity plan is evidence of that maturity.

It was also evident that existed two conflicting views on how outsourcing security contracts are celebrated in Portugal. On the one hand, contracts are specific enough to effectively regulate the IS security service and the relationship between client and

service provider. This point of view tends to see confidentiality, integrity, and availability as a premise of the service, enacted in the contract and without room for discussion on their contribution to a successful outsourcing relationship. The opposing view reports contracts as generic, with no specificity regarding information security and leaves to the service provider the responsibility of finding the scope of its service and almost self-regulating. As stated by participants, this may be the evidence of different maturity levels within organizations.

Another remark is that when participants confronted their own answers to the fourth round with the group's answer, almost without exception, they tended to relate their own choices with the ones of the group. In fact, items are not mutually exclusive and have some overlapping that cannot be excised. For example, trust can be related to credibility and the existence of previous relationships, and quality may be related to the competencies of human resources. Items also have different dimensions, which is to say, some items are more general than other. For example, trust seems wider than the existence of a business continuity plan.

Lastly, the interview inevitably led to discussing the realm of motivations of the client to outsource rather than on factors that can maintain or improve an outsourcing relationship from the point of view of the service provider.

5 COMPREHENSIVE ANALYSIS OF FINDINGS

As stated in the beginning of the dissertation, the objectives of this study were to identify the key issues leading to a successful IS security outsourcing relationship from the point of view of the provider and to rank these issues according to their perceived importance.

The first objective, which was to obtain a list of the most relevant issues, was pursued mainly in the first round and then refined over the subsequent rounds, which is to say that the blank sheet first round supplied the study with 25 issues that were then trimmed to 13 leading up to the fourth round, and following the stated preferences of the participants. These final 13 issues are presented in Table 5-1.

Table 5-1 – Final issues ranking.

Final Ranking	Issue Denomination
1	Clear definition of responsibilities of the client and of the IS security services provider
2	Credibility of the IS security services provider
3	Safeguard of the client's information confidentiality by the IS security service provider
4	Quality of services delivered by the IS security provider
5	Existing trust in the relationship between client and IS security services provider
6	Experience of the IS security provider in providing such services
7	Cost-benefit ratio of the IS security service from the client's point of view
8	Capability to evaluate the level of the IS security service performed
9	Response time of the IS security service provider
10	Evidence of the capability of the IS security services provider to perform the service in question

Final Ranking	Issue Denomination
11	Human resources competencies of the IS security services provider
12	Existence of a business continuity plan
13	Existence of successful previous relationships between the client and the service provider

The study accomplished the first objective satisfactorily. This is due to issues spanning a variety of subjects and also because they can be related to issues mentioned in the literature review. An analysis of where in the literature review the final issues are mentioned is presented in Table 5-2.

Table 5-2 – Analysis on where final ranking issues are mentioned in the literature review.

Final Ranking	Mentioned Where in Literature Review?
1	In Table 2-7, while describing top management support Tsohou et al. (2007) state that it is responsible for the timely and clear definition of responsibilities of employees of both organizations. Endorf (2004) states that managing IS security outsourcing includes defining roles and responsibilities. Alner (2001) also stresses the importance of defining responsibilities of client and service provider.
2	In Table 2-2, Nguyen et al. (2006) reference credibility as a condition for successful outsourcing relationships.
3	Fenn et al. (2002) state that outsourcing security might cause breaches of confidentiality. In Table 2-8 the same authors refer that the outsourcing contract should address data protection ensuring its confidentiality.
4	In Table 2-3 Nguyen et al. (2006) state that quality of the deliverables is relevant in managing the outsourcing relationship.

Final Ranking	Mentioned Where in Literature Review?
5	In Table 2-1, all authors except one, mention that trust is a key issue in an outsourcing relationship. In Table 2-3, Lee and Kim (1999) state that building a trust-based relationship is relevant in managing the outsourcing relationship.
6	In section 2.2.4 it is stated that analysing service providers should include their previous experience. Endorf (2004) in setting a procedure to identify good service providers, states that clients should confirm that providers have the experience being sought.
7	Fenn et al. (2002) state that there are potential cost savings in IS security outsourcing. Section 2.2.1 states that cost savings can be materialised through outsourcing. Endorf (2004) states that in determining which IS security functions to outsource a cost analysis should be performed.
8	–
9	Endorf (2004) in setting a general procedure to identify a good service provider states that one aspect to consider is the response time of the provider.
10	–
11	In section 2.7 it is stated that it has to be assured that the outsourcer has a well trained staff in the functions they would be performing.
12	–
13	Endorf (2004) in setting a general procedure to identify good service providers, states that current service providers the client is in business with should be considered.

It is then possible to conclude that from the 13 final issues, 10 had been mentioned in the literature review and were known as relevant to the IS outsourcing relationship. On the other hand, the existing literature focuses on the client side while this study focuses on the service provider side, thence it is possible to conclude that the majority of issues

are common to both sides but three issues (8, 10 and 12) seem specific to how service providers perceive the pursuit of a successful IS security relationship with the client. Two criticisms arise though: the first one deals with the fact that, even after being stressed constantly throughout the study that the intended point of view is the service providers', it became obvious in the interviews that some participants always default (maybe unknowingly) to the client's point of view. To them it is mainly a question of what the client is looking for in a service provider and what can they do to turn the decision in their favour. To a certain extent this makes sense, since the service providers' first goal is to stay in business and therefore have to think like the client in order to position themselves in the market. On the other hand, it makes it more difficult to understand which issues are specific to the provider. The second criticism deals with the fact that the issues have different dimensions (some are more abstract and seem to encompass more) and they are not completely independent from each other, triggering the participants to easily relate their most important issues to the group's most important issues.

The second objective was to rank the issues according to the relevance perceived by the group of participants. Here the results were not as satisfactory. Kendall's W (coefficient of concordance) receded round after round, even when fewer issues were being considered, showing a weak agreement between participants. There is no clear reason to why this happened. Volatility of the participants answers, usability of the Delphi tool used to administer the questionnaires, similarity or dependence between issues, the time taken to complete the four rounds of the questionnaires can all be waved but all without proof.

As a recommendation to future researchers pursuing this topic I would advise them to strive for two things: the first is to have face to face or telephone conversations with the participants after the first and second rounds. This, from my point of view, will align the participants with the objectives of the study, harvest their first opinions and help correct any misunderstandings towards the subject being researched or towards any methodological aspect of the study. It will probably also engage the participants in the study, weakening the probability of their withdrawal from it. The second thing the researcher should strive for is to decrease the time between rounds thus not dimming the bond the participants have with the study and with their own previous answers. This dimming bond can increase the volatility in the participants' answers and on the results of the study.

6 CONCLUSIONS

This study falls in the category of exploratory studies since no information relating to the service providers point of view in IS security outsourcing was found in the literature review and so this study treads new ground. This is increasingly important as outsourcing relationships tend to become more balanced and regarded as partnerships.
The stated objectives of the study were met through the development of a list of the 13 most important issues regarding the IS security outsourcing relationship, from the point of view of the service provider (Table 5-1) and also through the fact that it is a ranked list of issues. Regarding the ranking of issues, the agreement among the group is considered weak and so the second objective is only partially met.
In spite dwelling on a difficult subject, the study was successful. The argument for it being difficult comes from the fact that it is a largely unexplored domain in which there is no background to provide structure to ensuing works, and also because in the field of IS security it is typically hard to harvest information and practitioners tend to not be as forthcoming as they could be.
However the consolidated list of issues here compiled can certainly be a starting point to further studies dwelling on this same topic. It can be presented to experts in a Delphi first round, so they can agree or disagree with them, refine and resolve possible inconsistencies and interdependencies between them.
It would also be interesting to assess the clients' response to this list. Whether they agree or disagree and whether there is any item which stems any kind of discussion leading to a deeper understanding of the IS security outsourcing relationship.

Several issues have surfaced in the course of this study that may constitute work propositions to researchers intending to pursue the topic of IS security outsourcing or IS outsourcing at large.

A poignant issue is which aspects are paramount in winning the client and which are paramount in retaining the client and having a good ongoing relationship? Are they the same or overlap to some extent or are they even completely independent? Answering these questions would undoubtedly help understand which aspects are relevant in setting the relationship and then in maintaining it.

A second issue worth pursuing is the maturity level of organizations and how it conditions the success of outsourcing relationships. Can an organization that does not know itself well be successful in outsourcing any IS function? A related idea for further research would be to study to which extent is the price the dominant factor in resorting to outsourcing and how this relates to the maturity of the organization and its dependence on IS.

Another issue that emerged from this study is about the IS security outsourcing contract. Which is the *statu quo* of these contracts and are they generic or specific, helpful or not, and are they effective management tools or are just ignored?

Lastly, the dimension and overlapping of key issues was a topic of debate during this study's interviews. Would it be possible to develop a set of key issues balanced in their intrinsic dimension and independent?

These are questions worth pursuing.

REFERENCES

Alner, M., (2001), The Effects of Outsourcing on Information Security, *Information Security Journal: A Global Perspective*, 10, pp. 1-9.

Brancheau, J., Janz, B., Wetherbe, J. (1996), Key Issues in Information Systems Management: 1994-95 SIM Delphi Results, *MIS Quarterly*, 20, pp. 225-42.

Brancheau, J., Wetherbe, J. (1987), Key Issues in Information Systems Management, *MIS Quarterly*, 11, pp. 23-45.

Brown, S. (1993), A primer on Q methodology, *Operant Subjectivity*, 16, pp. 91-138.

Coase, R. (1937), The Nature of the Firm, *Econometrica*, 4, pp. 386-405.

Computer Security Institute (2009), 14th Annual CSI Computer Crime and Security Survey.

Dalkey, N., Helmer, O. (1963), An experimental application of the Delphi method to the use of experts, *Management Science*, 9, pp. 458-67.

Endorf, C. (2004), Outsourcing Security: The Need, the Risks, the Providers, and the Process, *Information Security Journal: A Global Perspective*, 12, pp. 17-23.

Ernst & Young (2009), Outpacing change: Ernst & Young's 12th annual global information security survey.

Fenn, C., Shooter, R., Allan, K. (2002), IT Security Outsourcing: how safe is your IT security?, *Computer Law & Security Report*, 18, pp. 109-111.

Goles, T., Chin, W. (2005), Information Systems Outsourcing Relationship Factors: Detailed Conceptualization and Initial Evidence, *The DATA BASE for Advances in Information Systems*, 36, pp. 47-67.

Green, B., Jones, M., Hughes, D., Williams, A. (1999), Applying the Delphi Technique in a Study of GP's Information Requirements, *Health and Social Care in the Community*, 7, pp. 198-205.

Grover, V., Cheon, M., Teng, J. (1996), The Effect of Service Quality and Partnership on the Outsourcing of Information Systems Functions, *Journal of Management Information Systems*, 12, pp. 89-116.

Hasson, F., Keeney, S., McKenna, H. (2000), Research guidelines for the Delphi survey technique, *Journal of Advanced Nursing*, 32, pp. 1008-15.

Holsapple, C., Joshi, K. (2002), Knowledge manipulation activities: results of a Delphi study, *Information & Management*, 39, pp. 477-90.

Kern, T. (1997), The Gestalt of an Information Technology Outsourcing Relationship: An Exploratory Analysis, *ICIS 1997 Proceedings*, Paper 3.

Kern, T., Willcocks, L. (2001), *The Relationship Advantage: Information Technologies, Sourcing, and Management*, Oxford: Oxford University Press.

Ketler, K., Willems, J. (1999), A study of the outsourcing decision: preliminary results, *Proceedings of the 1999 ACM SIGCPR conference on Computer personnel research*, 182-189.

Lee, J., Huynh, M., Kwok, R., Pi, S. (2003), IT Outsourcing Evolution – Past, Present and Future, *Communications of the ACM*, 46, pp. 84-89.

Lee, J., Kim, Y. (1999), Effect of Partnership Quality on IS Outsourcing Success: Conceptual Framework and Empirical Validation. *Journal of Management Information Systems*, 15, pp. 29-61.

Linstone, H., Turoff, M. (1975), *The Delphi Method: Techniques and Applications*, London: Addison-Wesley.

McFarlan, F., Nolan, R. (1995), How to Manage an IT Outsourcing Alliance, *Sloan Management Review*, 36, pp. 9-23.

McKenna, H. (1994), The Delphi technique: a worthwhile approach for nursing?, *Journal of Advanced Nursing*, 19, pp. 1221-1225.

Nam, K., Rajagopalan, S., Rao, H., Chaudury, A. (1996), A Two-Level Investigation of Information Systems Outsourcing, *Communications of the ACM*, 39, pp. 36-44.

Nambisan, S., Agarwal, R., Tanniru, M. (1999), Organizational mechanisms for enhancing user innovation in information technology, *MIS Quarterly*, 23, pp. 365-395.

Nguyen, P., Babar, M., Verner, J. (2006), Critical Factors in Establishing and Maintaining Trust in Software Outsourcing Relationships, *Proceedings of the 28th international conference on Software engineering*, pp. 624-627.

Okoli, C., Pawlowski, S. (2004), The Delphi method as a research tool: an example, design considerations and applications, *Information & Management*, 42, pp. 15-29.

Power, R., Forte, D., (2005), Outsourced or outsmarted? Part II: security outsourcing issues, *Computer Fraud & Security*, 2005, pp. 17-20.

Rowe, B., (2007), Outsourcing IT Security Leads to a Higher Social Level of Security?, 2007 *Workshop on the Economics of Information Security*.

Santos, L., Amaral, L. (2004), Estudos Delphi com Q-Sort sobre a web - A sua utilização em Sistemas de Informação, Proceedings of the *Conferência da Associação Portuguesa de Sistemas de Informação 2004*.

Schmidt, R. (1997), Managing Delphi surveys using nonparametric statistical techniques, *Decision Sciences*, 28, pp. 763-774.

Schmidt, R., Lyytinen, K., Keil, M., Cule, P. (2001), Identifying software project risks: an international Delphi study, *Journal of Management Information Systems,* 17, pp. 5-36.

Schneier, B., (2002), The case for outsourcing security, *Computer*, 35, pp. 20-26.

Tsohou, A., Theoharidou, M., Kokolakis, S., Gritzalis, D. (2007), Addressing cultural dissimilarity in the Information Security Management Outsourcing relationship, *Trust, Privacy and Security in Digital Business*, 4657, pp. 24-33.

Turoff, M. (1970), The design of a policy Delphi, *Technological Forecasting and Social Change*, 2, pp. 149-171.

Van Exel, J., de Graaf, G. (2005), Q methodology: A sneak preview, http://www.qmethodology.net/PDF/Q-methodology%20-%20A%20sneak%20preview.pdf [Accessed Jan 27 2010].

Williams, P., Webb, C. (1994), The Delphi technique: a methodological discussion, *Journal of Advanced Nursing*, 19, pp. 180-186.

Whitman, N. (1990), The committee meeting alternative: using the Delphi technique, *Journal of Nursing Administration,* 20, pp. 30-37.

ANNEX A. ROUND RESULTS

Annex A presents the lists of issues that were the outcome of each Delphi round. It starts by presenting the consolidated list of issues obtained in the first round and then goes on to present the ordered list of issues resultant of each round, ranked by importance.

Table A-1 – Consolidated list of issues

Issue	Denomination	Description
1	Existing trust in the relationship between client and IS security services provider	It refers to the relationship of trust existing between the two parties, including the technical capabilities of the service provider to deliver the service and its financial viability, in order to minimize the possibility of the provider exiting the market and leaving the client in a difficult situation.
2	Credibility of the IS security services provider	It refers to the credible and capable way in which the IS service provider is perceived by the client.
3	Cost-benefit ratio of the IS security service from the client's point of view	It refers to the fact that the IS security service performed by the service provider should have a cost-benefit ratio favorable to the client to make him prefer the outsourcing solution to an internal one. The ratio can also be favorable to the client because it enables him to decrease the costs with human resources, contracted infrastructures and level of service obtained.
4	Clear definition of responsibilities of the client and of the IS security services provider	It refers to the clear definition (if possible, written in the contract) of which are the responsibilities of the client and which are the responsibilities of the service provider as to the definition and operation of the security requirements, as well as to the scope of action/role of each party of the outsourcing partnership.
5	Commitment by the IS security	It refers to the commitment on the part of the service

Issue	Denomination	Description
	services provider to continuously improve the service performed	provider to continuously improve the performed service, in order to justify, continuously, the cost-benefit ratio of outsourcing.
6	Evidence of the capability of the IS security services provider to perform the service in question	It refers to the possibility of checking, for example, through holding an ISO 27001 certification, that the service provider has the required capability to perform the IS security services in question.
7	Guarantee of non-repudiation of tasks performed by the IS security services provider	It refers to obtaining unequivocal guarantees of non-repudiation of tasks that were performed by the IS security service provider.
8	Security services diversity of offer by the service provider	It refers to how large the portfolio of services offered by the service provider is, supposing that the bigger and wider it is the higher the probability of being hired by the client to provide a global solution with costs comparatively smaller.
9	Communication channels between the client and the IS security provider	It refers to procedures and communication means to be used in the various situations of service providing, either in the normal operational situations or in crisis situations (security incident, service level decrease, etc.).
10	Knowledge by the IS security service provider of the market in which the client operates	It refers to the knowledge the information security service provider has of the market in which the client organization operates, namely in relation to possible security risks the client's business might face.
11	Existence of successful previous relationships between the client and the service provider	It refers to the existence of prior relationships between the service provider and the client that allow to know the culture, the processes, the procedures, the IS and the people of both sides of the outsourcing partnership.
12	Unequivocal identification of who is executing tasks within the scope of the IS security service	It refers to the unequivocal identification of the human resources from the service provider authorized to execute tasks within the scope of the IS security service provided.
13	Human resources competencies of the IS security services provider	It refers to the necessity of human resources composing the teams of the IS service provider to congregate technical

Issue	Denomination	Description
		competencies (hard skills) such as technical knowledge, certifications, etc., together with non-technical competencies (soft skills) such as relationship building, management capabilities, etc.
14	Execution and management method of the IS security service	It refers to the method, applied by the service provider but accepted by both parties, to execute and manage the IS security service (service catalogue, available tasks, strategy, etc.).
15	Support in complying with requirements, regulatory or legal, by the IS security service provider	It refers to the specialized support the IS security service provider may deliver to the client organization in order for it to comply with legal or regulatory requirements.
16	Experience of the IS security provider in providing such services	It refers to the experience the market recognizes in the IS security services provider in delivering such services.
17	Safeguard of the client's information confidentiality by the IS security service provider	It refers to the guarantees given by the IS security outsourcing service provider regarding the confidentiality of the client's information, disallowing its unlawful disclosure and sharing.
18	Shared management of IS security between the client and the service provider	It refers to the necessity of a joint management of IS security by both parties of the outsourcing relationship, not leaving to the client all the responsibility for managing information security.
19	Capability to evaluate the level of the IS security service performed	It refers to the possibility of assessing the cost-benefit ratio of the outsourcing service delivered, by which it is mandatory to define clear methods and metrics (for example, SLA) to measure, control and audit the provided outsourcing service.
20	Quality of services delivered by the IS security provider	It refers to the quality of the services performed by the IS security service provider from the point of view of complying with the requirements initially contracted by the client.
21	Increased focus of the client in its	It refers to the fact that the outsourcing of IS security allows

Issue	Denomination	Description
	business requirements and strategy	the client to focus harder on the nuclear activities of his business.
22	Existence of a business continuity plan	It refers to the existence of a business continuity plan which the IS provider is responsible for, and that includes procedures to deal with incidents and disaster recovery.
23	Response time of the IS security service provider	It refers to the availability of the IS security service provider to answer with a promptness that matches the gravity of what occurred to the information assets whose security was outsourcing.
24	Compatibility between the organizational cultures of the two sides of the outsourcing partnership	It refers to the compatibility, or possibility of adaptation, between the culture of the client organization and that of the IS security service provider organization.
25	Decrease of the operational cost for the IS security provider	It refers to employing technological solutions that enable the IS security service provider to reduce its operational costs of supporting the service, such as the possibility of performing an intervention remotely and also employing stable technological solutions less prone to problems.

Table A-2 – Issues ranking after the second round

Rank: 2nd Round	Issue Denomination	Mean	Standard Deviation
1	Evidence of the capability of the IS security services provider to perform the service in question	8,10	5,53
2	Credibility of the IS security services provider	8,30	7,48
3	Experience of the IS security provider in providing such services	8,50	6,52
4	Existing trust in the relationship between client and IS security services provider	8,70	7,12
5	Clear definition of responsibilities of the client and of the IS security services provider	9,10	5,15

Rank: 2nd Round	Issue Denomination	Mean	Standard Deviation
6	Existence of successful previous relationships between the client and the service provider	9,20	6,23
7	Execution and management method of the IS security service	10,40	7,47
8	Safeguard of the client's information confidentiality by the IS security service provider	10,60	6,40
9	Capability to evaluate the level of the IS security service performed	10,70	6,80
10	Quality of services delivered by the IS security provider	10,80	4,85
11	Communication channels between the client and the IS security provider	11,80	6,34
12	Cost-benefit ratio of the IS security service from the client's point of view	12,00	7,41
13	Response time of the IS security service provider	12,50	6,20
14	Support in complying with requirements, regulatory or legal, by the IS security service provider	12,90	7,31
15	Existence of a business continuity plan	15,00	6,80
16	Shared management of IS security between the client and the service provider	15,10	7,13
17	Human resources competencies of the IS security services provider	15,40	7,06
18	Unequivocal identification of who is executing tasks within the scope of the IS security service	15,40	7,49
19	Increased focus of the client in its business requirements and strategy	15,50	7,41
20	Decrease of the operational cost for the IS security provider	15,70	7,87
21	Compatibility between the organizational cultures of the two sides of the outsourcing partnership	15,80	6,83
22	Guarantee of non-repudiation of tasks performed by the IS security services provider	17,20	7,80
23	Knowledge by the IS security service provider of the market in which the client operates	17,80	4,85
24	Security services diversity of offer by the service provider	19,10	6,49
25	Commitment by the IS security services provider to continuously improve the service performed	19,40	4,43

Table A-3 - Issues ranking after the third round

Rank: 3rd Round	Issue Denomination	Mean	Standard Deviation
1	Clear definition of responsibilities of the client and of the IS security services provider	8,11	5,84
2	Execution and management method of the IS security service	8,22	3,93
3	Experience of the IS security provider in providing such services	8,22	4,87
4	Quality of services delivered by the IS security provider	8,22	6,78
5	Evidence of the capability of the IS security services provider to perform the service in question	8,33	6,86
6	Safeguard of the client's information confidentiality by the IS security service provider	8,67	4,66
7	Shared management of IS security between the client and the service provider	9,11	5,73
8	Cost-benefit ratio of the IS security service from the client's point of view	9,11	6,88
9	Capability to evaluate the level of the IS security service performed	9,67	6,28
10	Credibility of the IS security services provider	9,89	4,31
11	Existence of a business continuity plan	10,00	5,72
12	Existing trust in the relationship between client and IS security services provider	10,67	4,47
13	Response time of the IS security service provider	11,33	3,84
14	Human resources competencies of the IS security services provider	11,89	5,35
15	Communication channels between the client and the IS security provider	12,44	5,32
16	Unequivocal identification of who is executing tasks within the scope of the IS security service	12,56	5,50
17	Existence of successful previous relationships between the client and the service provider	12,67	6,22
18	Increased focus of the client in its business requirements and strategy	13,00	5,27
19	Support in complying with requirements, regulatory or legal, by the IS security service provider	13,67	7,71
20	Decrease of the operational cost for the IS security provider	14,22	7,16

Table A-4 - Issues ranking after the fourth round

Rank: 4th Round	Issue Denomination	Mean	Standard Deviation
1	Clear definition of responsibilities of the client and of the IS security services provider	4,11	4,14
2	Credibility of the IS security services provider	5,56	3,00
3	Safeguard of the client's information confidentiality by the IS security service provider	6,44	3,24
4	Quality of services delivered by the IS security provider	6,67	2,92
5	Existing trust in the relationship between client and IS security services provider	6,67	3,35
6	Experience of the IS security provider in providing such services	6,78	3,35
7	Cost-benefit ratio of the IS security service from the client's point of view	6,78	5,59
8	Capability to evaluate the level of the IS security service performed	7,00	2,40
9	Response time of the IS security service provider	7,33	3,46
10	Evidence of the capability of the IS security services provider to perform the service in question	7,44	4,13
11	Human resources competencies of the IS security services provider	8,11	4,08
12	Existence of a business continuity plan	8,44	4,00
13	Existence of successful previous relationships between the client and the service provider	9,67	3,74

ANNEX B. BOX PLOTS OF THE FOURTH ROUND

Annex B presents the box plots for the dispersion of answers of experts to a certain issue in the fourth round.

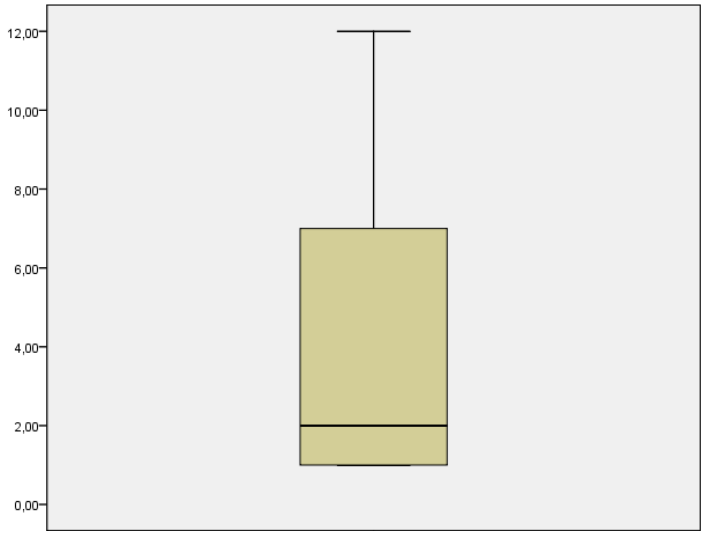


Figure B-1 - Clear definition of responsibilities of the client and of the IS security services provider

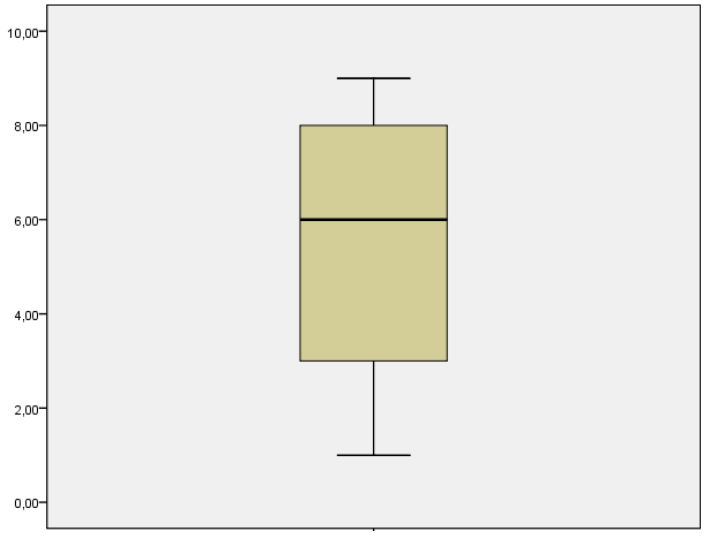


Figure B-2 - Credibility of the IS security services provider

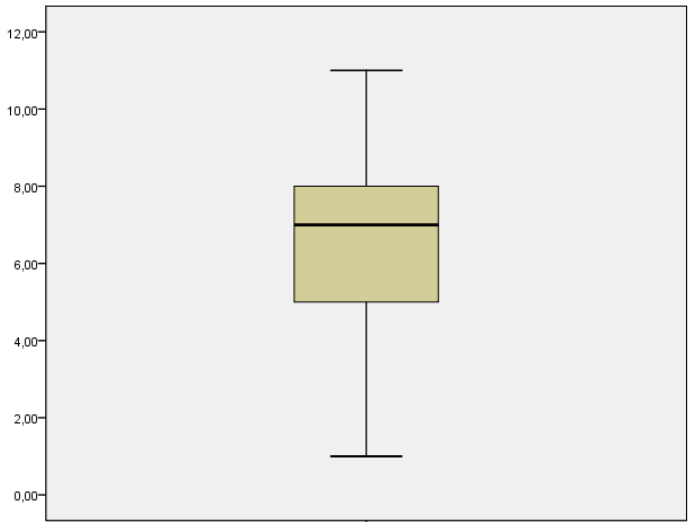


Figure B-3 - Safeguard of the client's information confidentiality by the IS security service provider

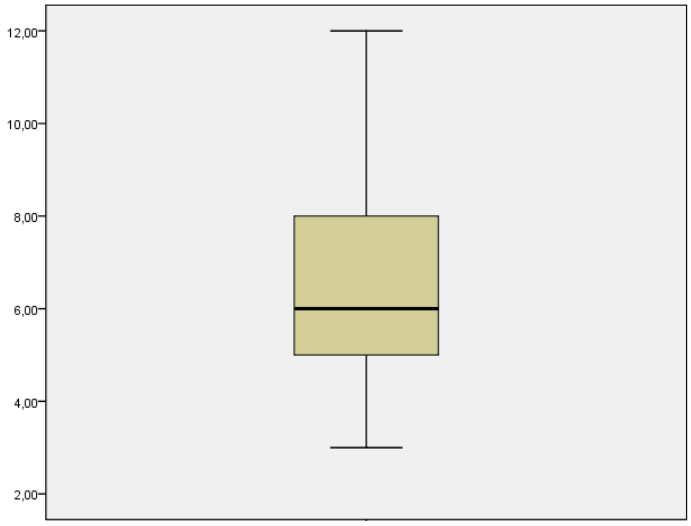


Figure B-4 - Quality of services delivered by the IS security provider

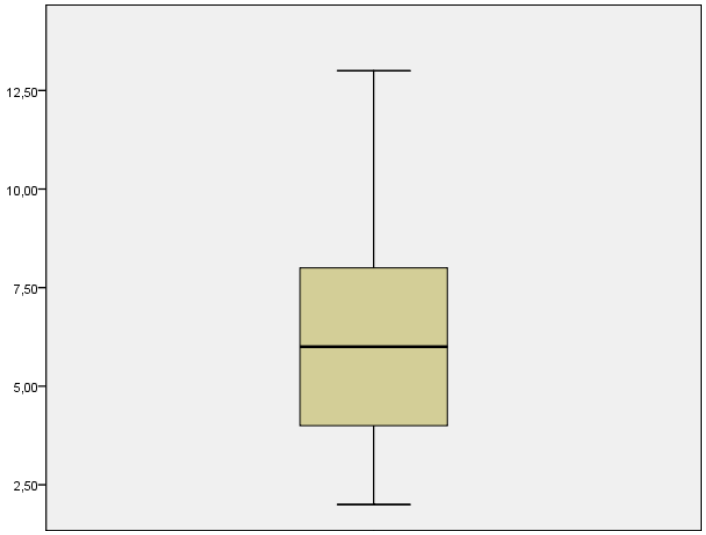


Figure B-5 - Existing trust in the relationship between client and IS security services provider

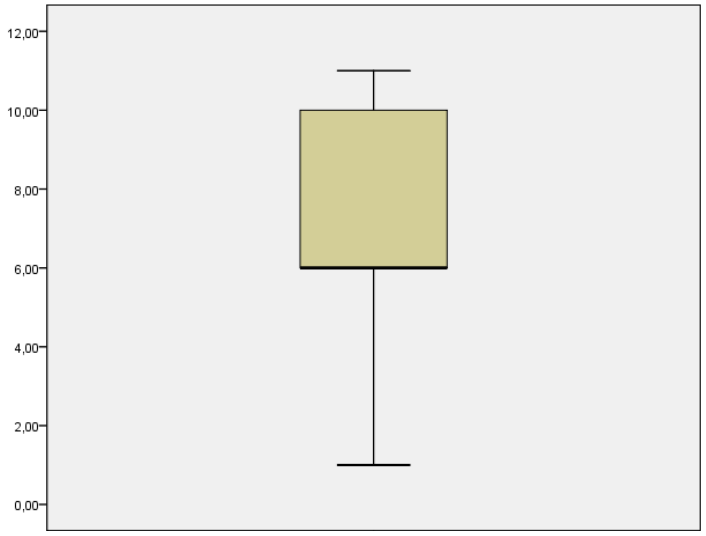


Figure B-6 - Experience of the IS security provider in providing such services

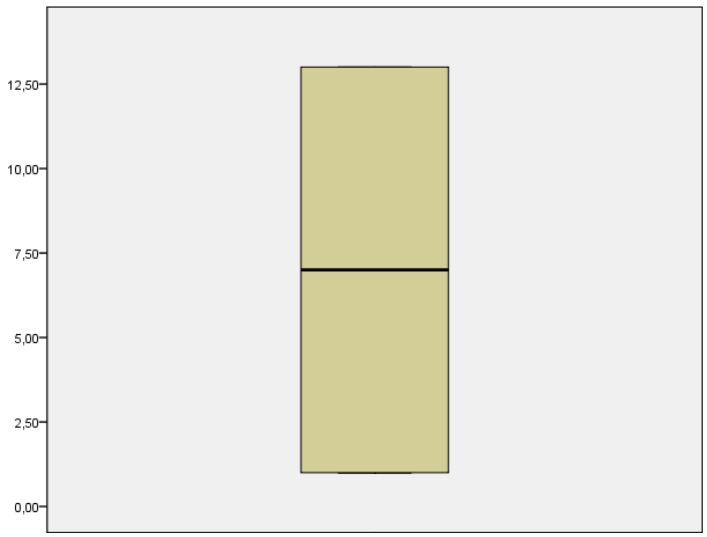


Figure B-7 - Cost-benefit ratio of the IS security service from the client's point of view

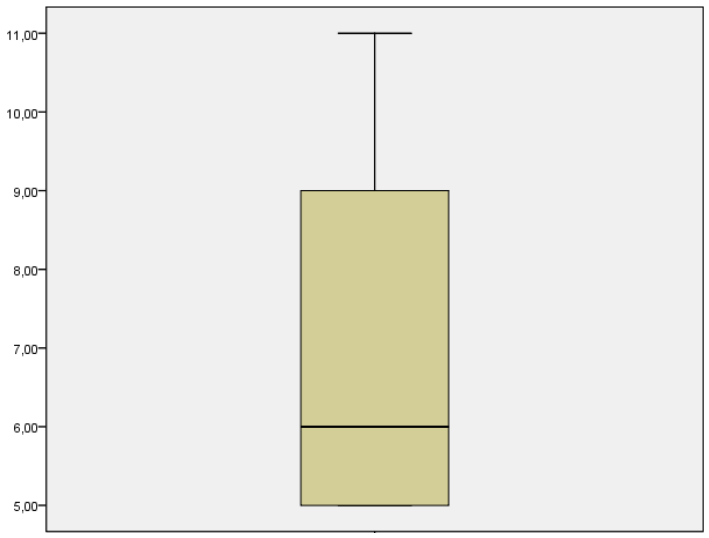


Figure B-8 - Capability to evaluate the level of the IS security service performed

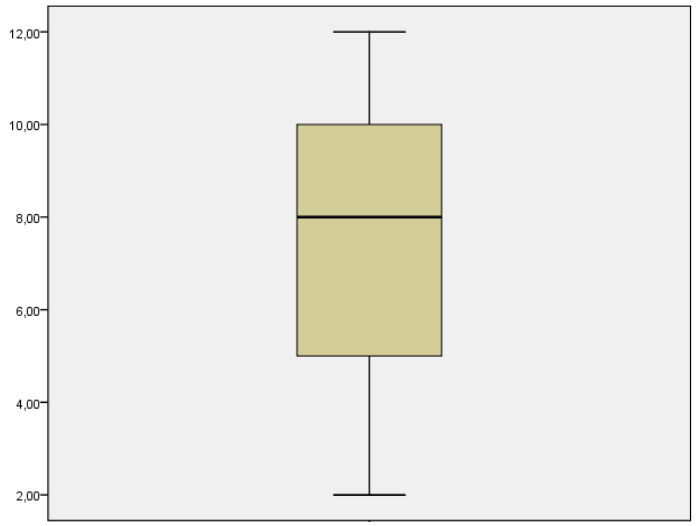


Figure B-9 - Response time of the IS security service provider

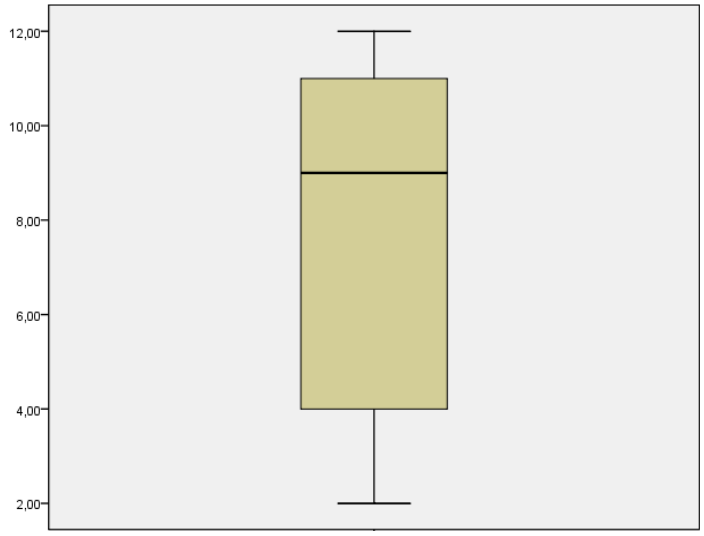


Figure B-10 - Evidence of the capability of the IS security services provider to perform the service in question

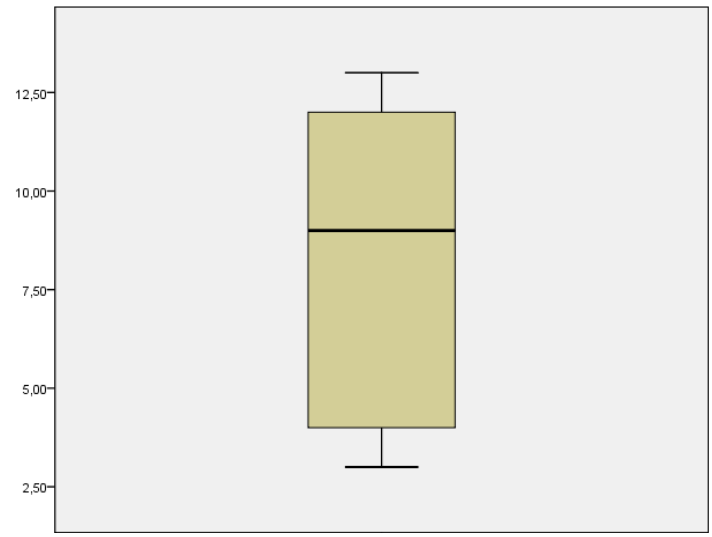


Figure B-11 - Human resources competencies of the IS security services provider

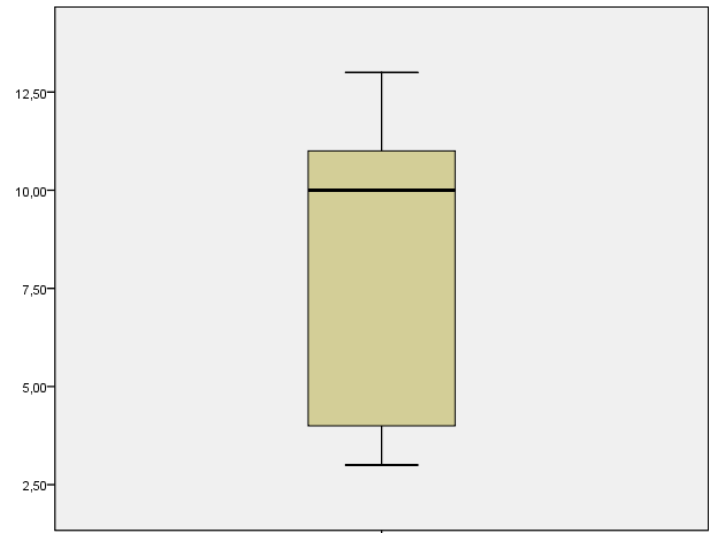


Figure B-12 - Existence of a business continuity plan

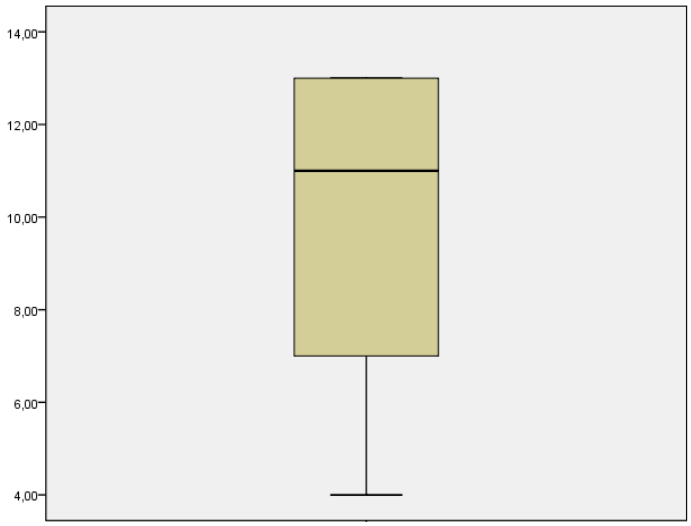
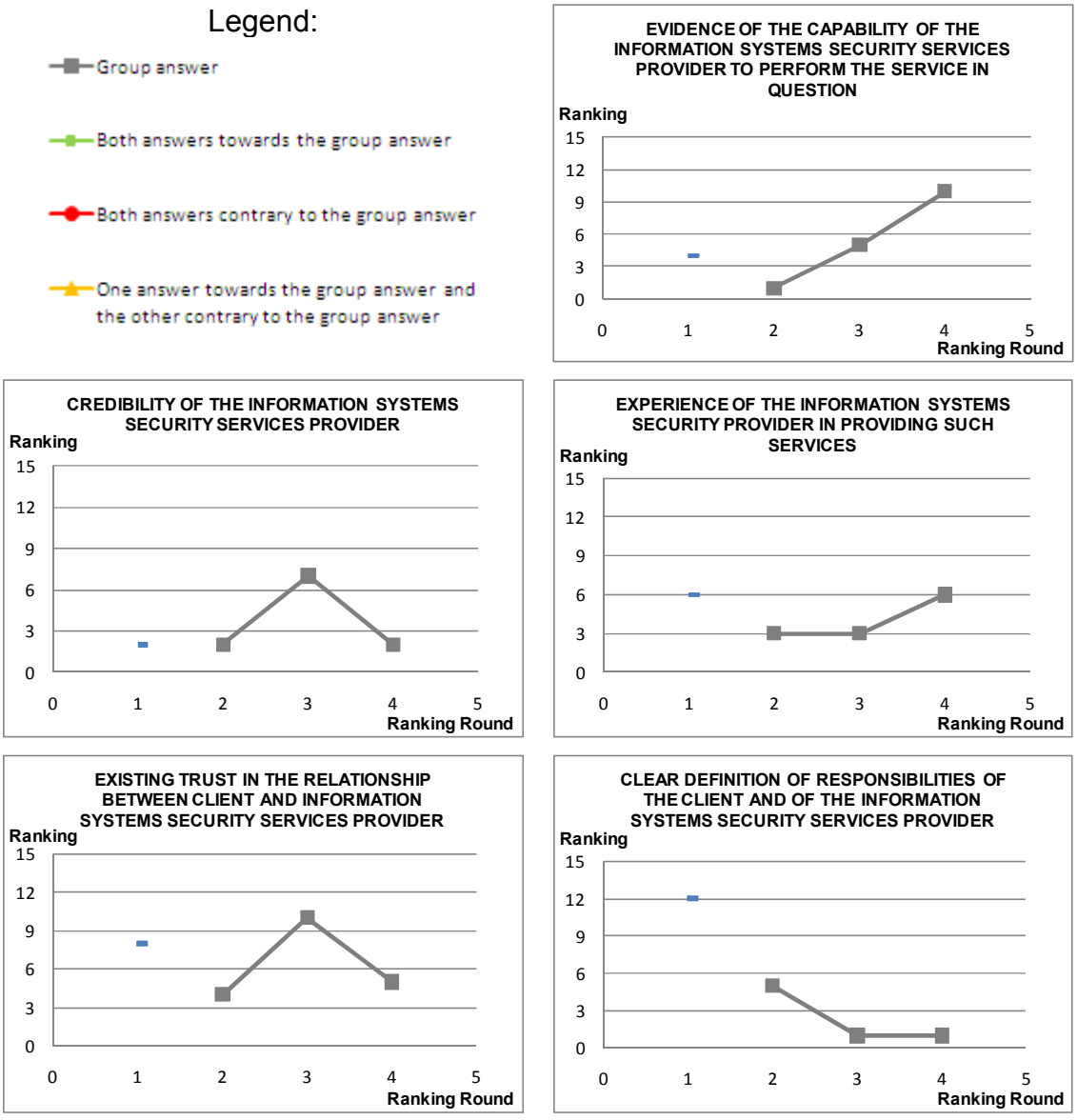


Figure B-13 – Existence of successful previous relationships between the client and the service provider

ANNEX C. PARTICIPANTS ANSWERS

For each participant and for each issue a plot is presented comparing the answers given by the expert in question with the group' answers.



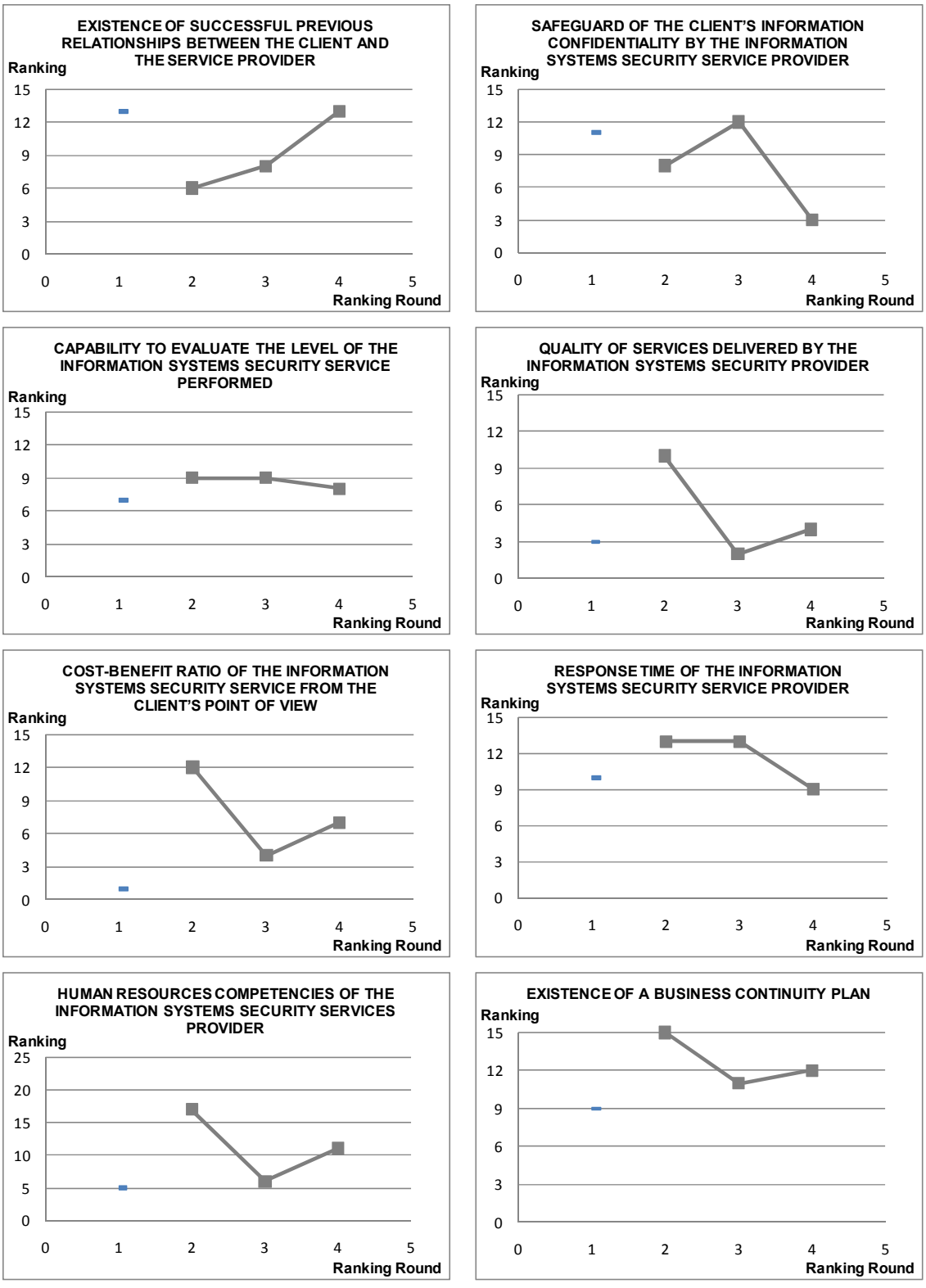
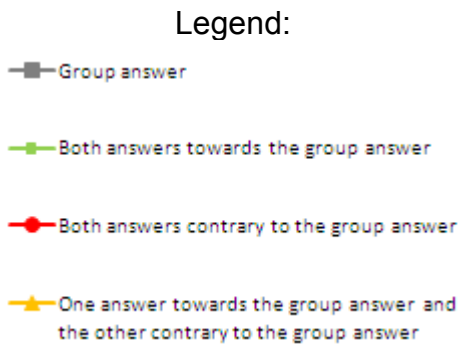
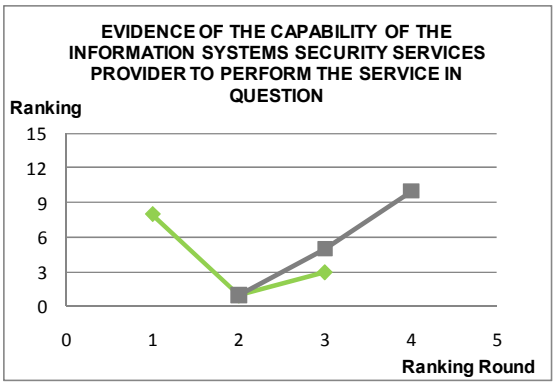
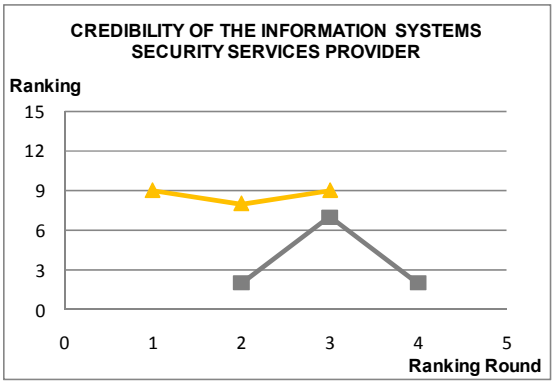
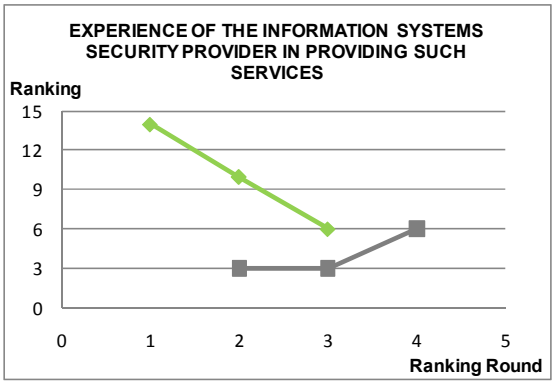


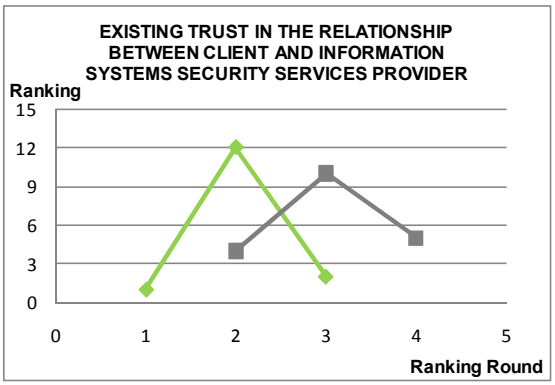
Figure C-1 – Round Answers from Participant [P1]

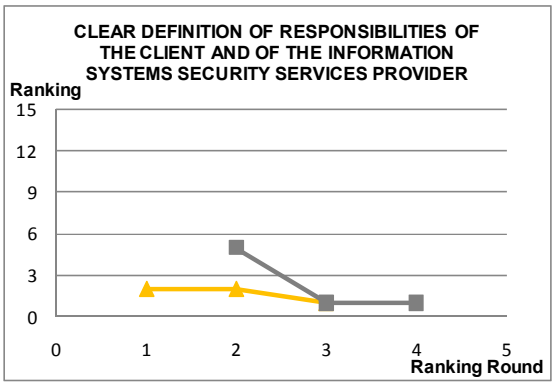

Legend:
Group answer
Both answers towards the group answer
Both answers contrary to the group answer
One answer towards the group answer and the other contrary to the group answer

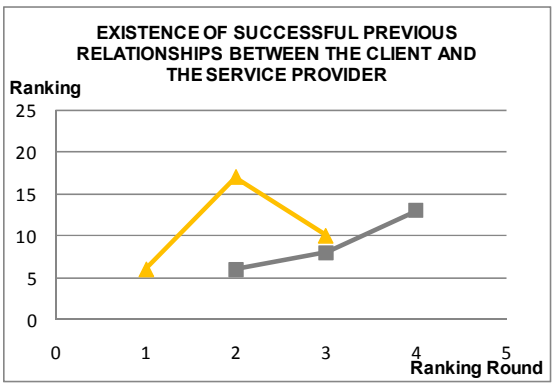

EVIDENCE OF THE CAPABILITY OF THE INFORMATION SYSTEMS SECURITY SERVICES PROVIDER TO PERFORM THE SERVICE IN QUESTION
Ranking
15
12
9
6
3
0
0 1 2 3 4 5
Ranking Round

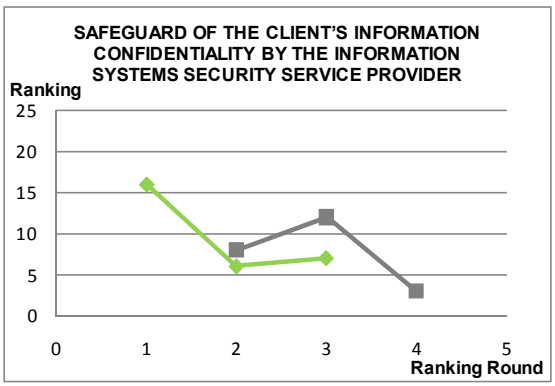

CREDIBILITY OF THE INFORMATION SYSTEMS SECURITY SERVICES PROVIDER
Ranking
15
12
9
6
3
0
0 1 2 3 4 5
Ranking Round


EXPERIENCE OF THE INFORMATION SYSTEMS SECURITY PROVIDER IN PROVIDING SUCH SERVICES
Ranking
15
12
9
6
3
0
0 1 2 3 4 5
Ranking Round


EXISTING TRUST IN THE RELATIONSHIP BETWEEN CLIENT AND INFORMATION SYSTEMS SECURITY SERVICES PROVIDER
Ranking
15
12
9
6
3
0
0 1 2 3 4 5
Ranking Round


CLEAR DEFINITION OF RESPONSIBILITIES OF THE CLIENT AND OF THE INFORMATION SYSTEMS SECURITY SERVICES PROVIDER
Ranking
15
12
9
6
3
0
0 1 2 3 4 5
Ranking Round


EXISTENCE OF SUCCESSFUL PREVIOUS RELATIONSHIPS BETWEEN THE CLIENT AND THE SERVICE PROVIDER
Ranking
25
20
15
10
5
0
0 1 2 3 4 5
Ranking Round


SAFEGUARD OF THE CLIENT'S INFORMATION CONFIDENTIALITY BY THE INFORMATION SYSTEMS SECURITY SERVICE PROVIDER
Ranking
25
20
15
10
5
0
0 1 2 3 4 5
Ranking Round

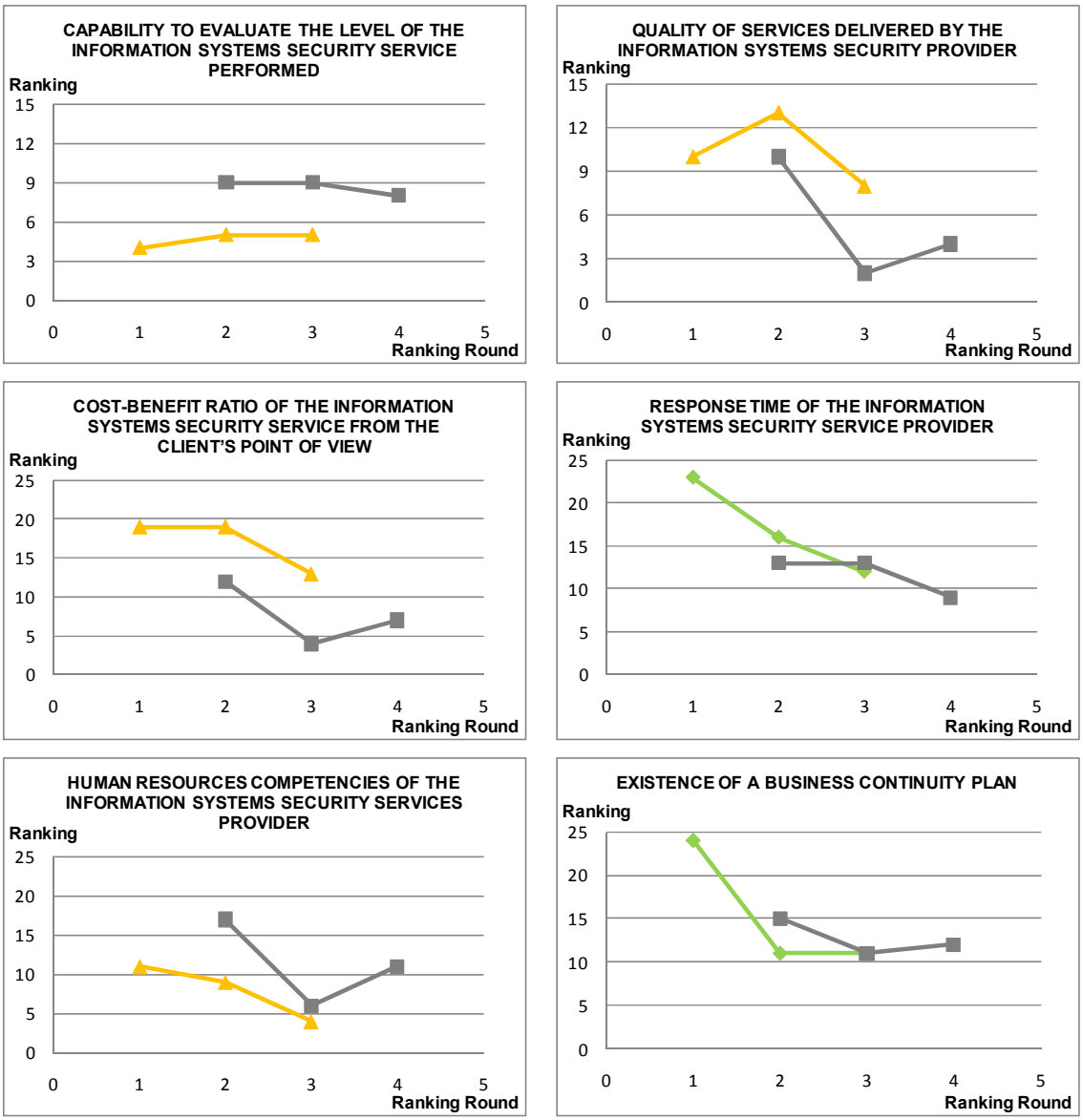
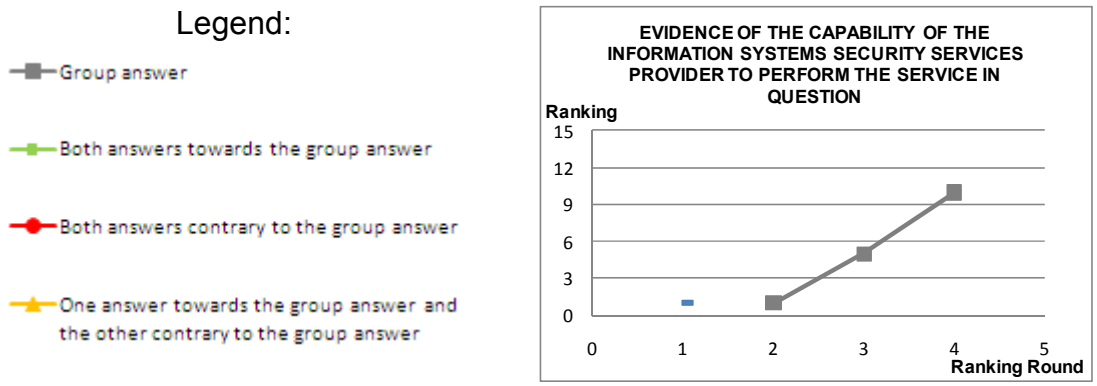
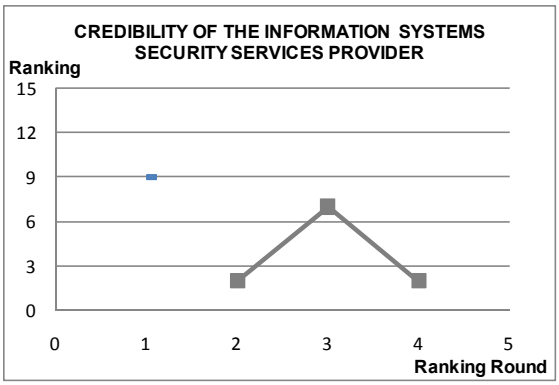
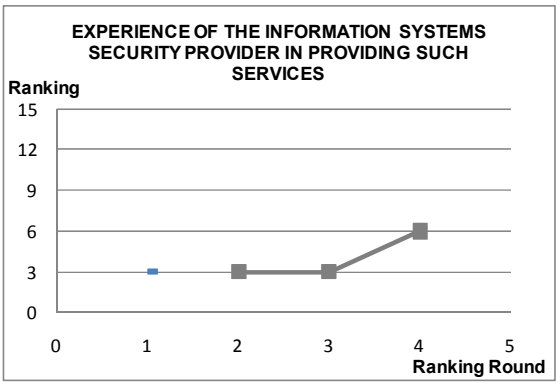
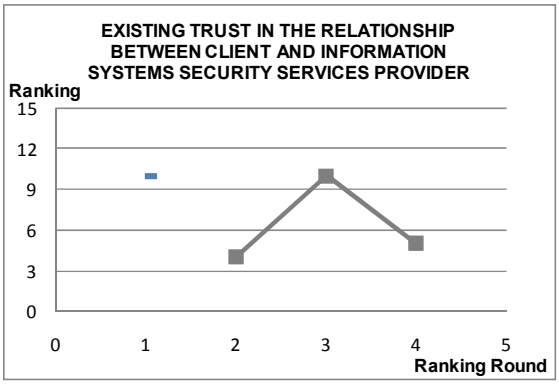


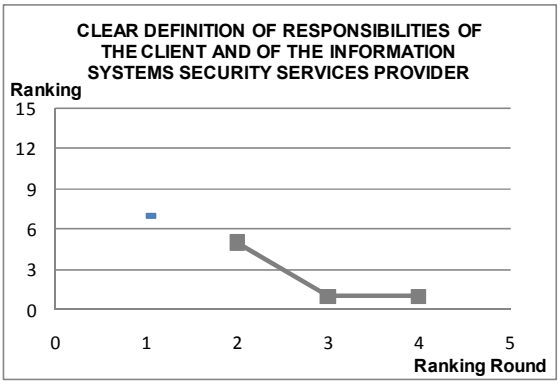
Figure C- 2 – Round Answers from Participant [P3]

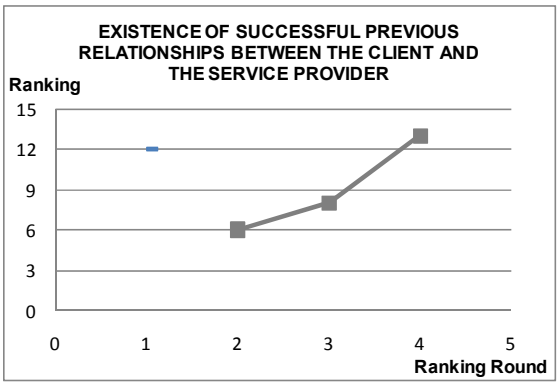


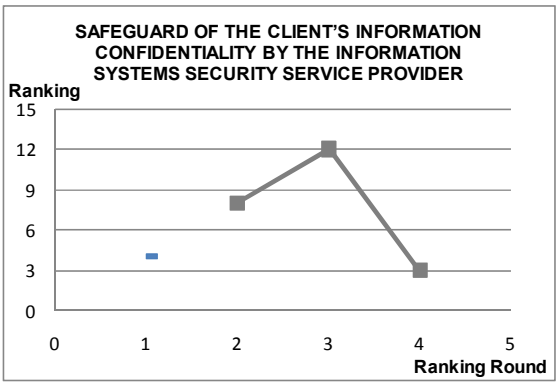

CREDIBILITY OF THE INFORMATION SYSTEMS SECURITY SERVICES PROVIDER
Ranking
15
12
9
6
3
0
0 1 2 3 4 5
Ranking Round

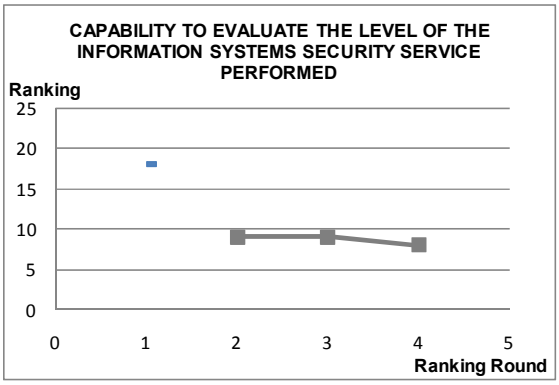

EXPERIENCE OF THE INFORMATION SYSTEMS SECURITY PROVIDER IN PROVIDING SUCH SERVICES
Ranking
15
12
9
6
3
0
0 1 2 3 4 5
Ranking Round

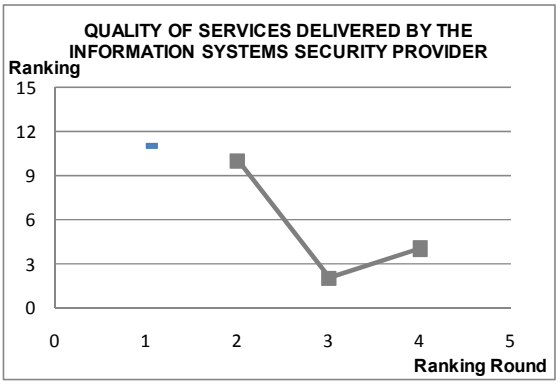

EXISTING TRUST IN THE RELATIONSHIP BETWEEN CLIENT AND INFORMATION SYSTEMS SECURITY SERVICES PROVIDER
Ranking
15
12
9
6
3
0
0 1 2 3 4 5
Ranking Round


CLEAR DEFINITION OF RESPONSIBILITIES OF THE CLIENT AND OF THE INFORMATION SYSTEMS SECURITY SERVICES PROVIDER
Ranking
15
12
9
6
3
0
0 1 2 3 4 5
Ranking Round


EXISTENCE OF SUCCESSFUL PREVIOUS RELATIONSHIPS BETWEEN THE CLIENT AND THE SERVICE PROVIDER
Ranking
15
12
9
6
3
0
0 1 2 3 4 5
Ranking Round


SAFEGUARD OF THE CLIENT'S INFORMATION CONFIDENTIALITY BY THE INFORMATION SYSTEMS SECURITY SERVICE PROVIDER
Ranking
15
12
9
6
3
0
0 1 2 3 4 5
Ranking Round


CAPABILITY TO EVALUATE THE LEVEL OF THE INFORMATION SYSTEMS SECURITY SERVICE PERFORMED
Ranking
25
20
15
10
5
0
0 1 2 3 4 5
Ranking Round


QUALITY OF SERVICES DELIVERED BY THE INFORMATION SYSTEMS SECURITY PROVIDER
Ranking
15
12
9
6
3
0
0 1 2 3 4 5
Ranking Round

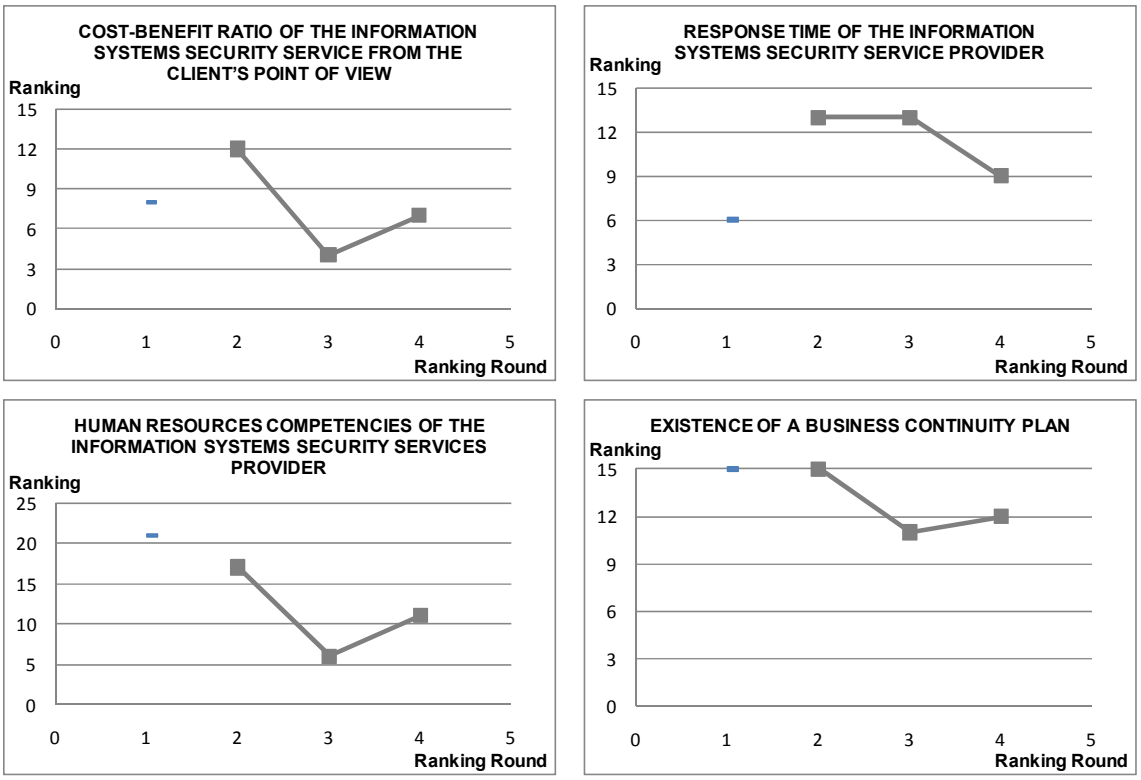
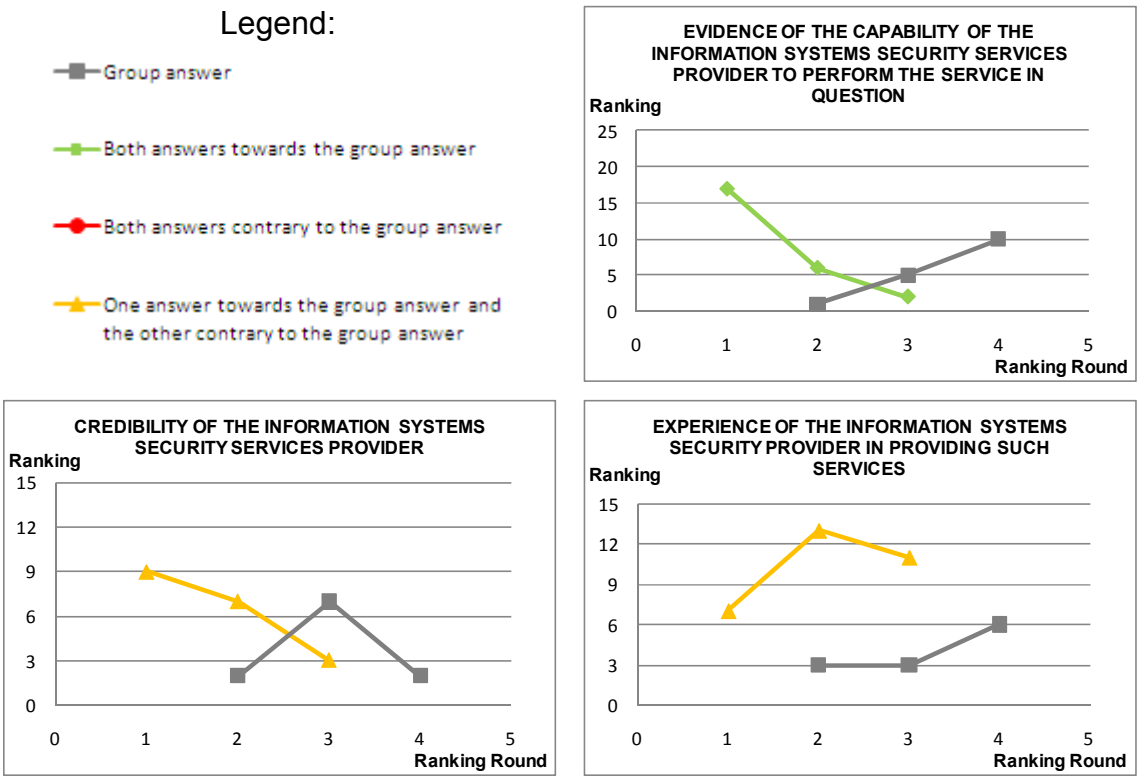
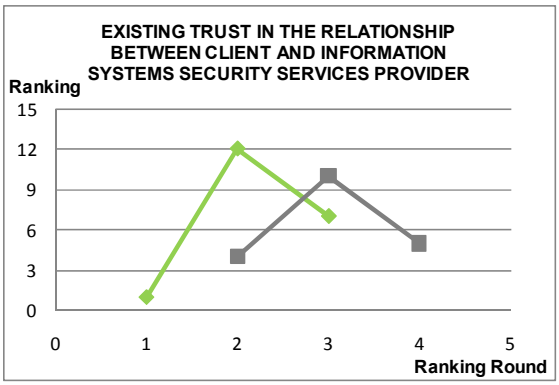
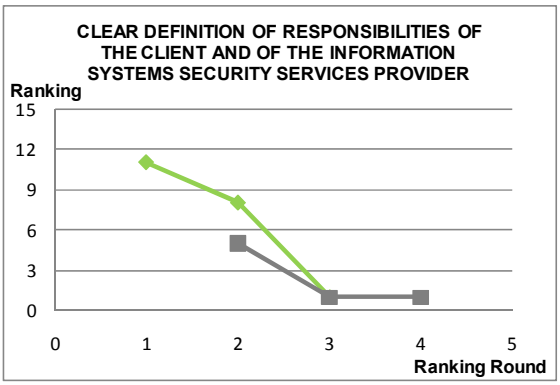
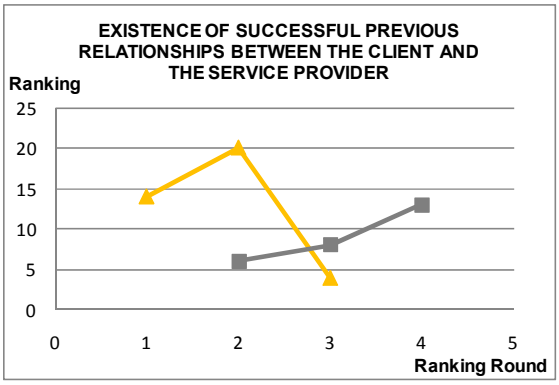


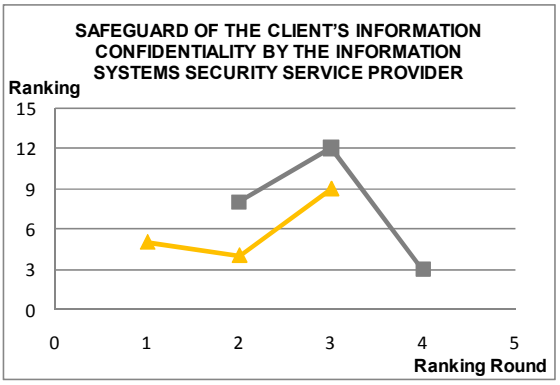
Figure C-3 – Round Answers from Participant [P4]

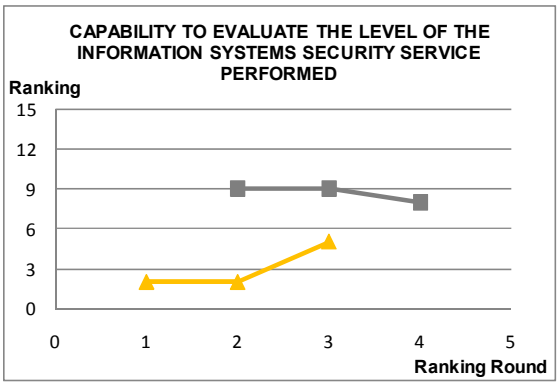


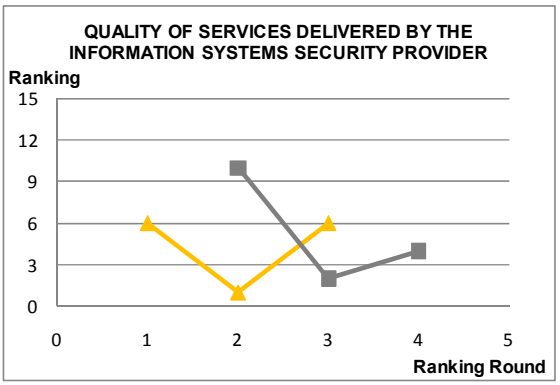

EXISTING TRUST IN THE RELATIONSHIP BETWEEN CLIENT AND INFORMATION SYSTEMS SECURITY SERVICES PROVIDER
Ranking
15
12
9
6
3
0
0 1 2 3 4 5
Ranking Round

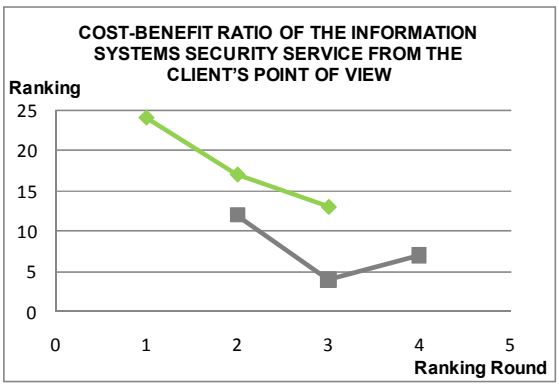

CLEAR DEFINITION OF RESPONSIBILITIES OF THE CLIENT AND OF THE INFORMATION SYSTEMS SECURITY SERVICES PROVIDER
Ranking
15
12
9
6
3
0
0 1 2 3 4 5
Ranking Round

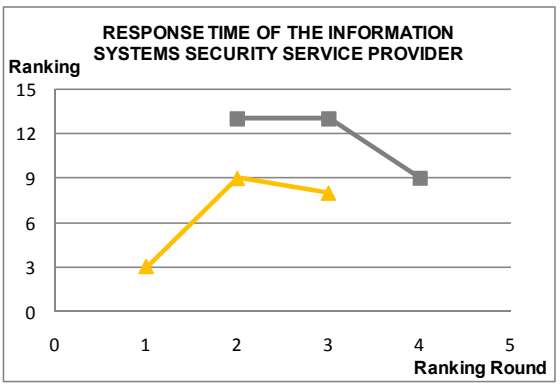

EXISTENCE OF SUCCESSFUL PREVIOUS RELATIONSHIPS BETWEEN THE CLIENT AND THE SERVICE PROVIDER
Ranking
25
20
15
10
5
0
0 1 2 3 4 5
Ranking Round

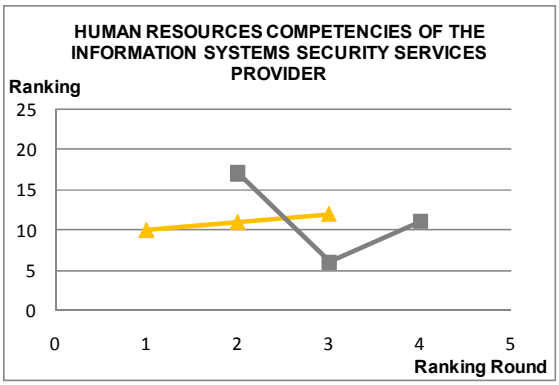

SAFEGUARD OF THE CLIENT'S INFORMATION CONFIDENTIALITY BY THE INFORMATION SYSTEMS SECURITY SERVICE PROVIDER
Ranking
15
12
9
6
3
0
0 1 2 3 4 5
Ranking Round


CAPABILITY TO EVALUATE THE LEVEL OF THE INFORMATION SYSTEMS SECURITY SERVICE PERFORMED
Ranking
15
12
9
6
3
0
0 1 2 3 4 5
Ranking Round


QUALITY OF SERVICES DELIVERED BY THE INFORMATION SYSTEMS SECURITY PROVIDER
Ranking
15
12
9
6
3
0
0 1 2 3 4 5
Ranking Round


COST-BENEFIT RATIO OF THE INFORMATION SYSTEMS SECURITY SERVICE FROM THE CLIENT'S POINT OF VIEW
Ranking
25
20
15
10
5
0
0 1 2 3 4 5
Ranking Round


RESPONSE TIME OF THE INFORMATION SYSTEMS SECURITY SERVICE PROVIDER
Ranking
15
12
9
6
3
0
0 1 2 3 4 5
Ranking Round



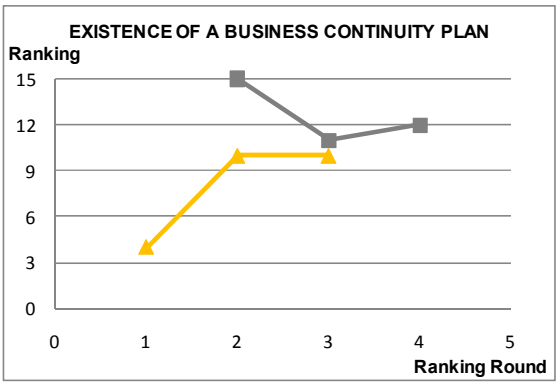
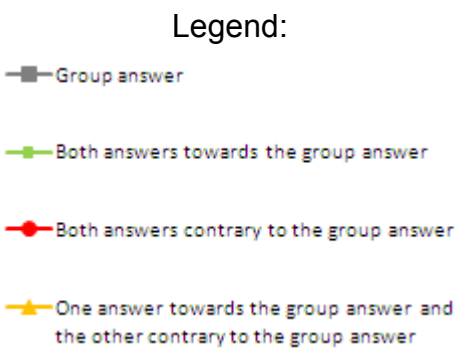
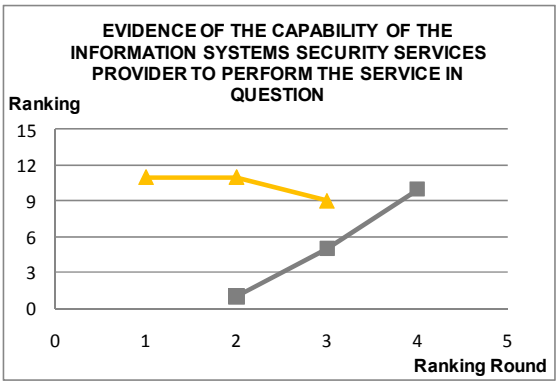
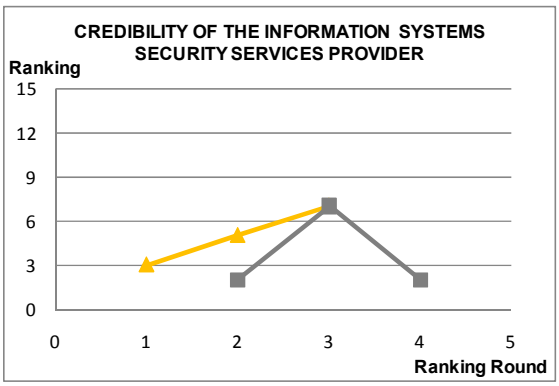
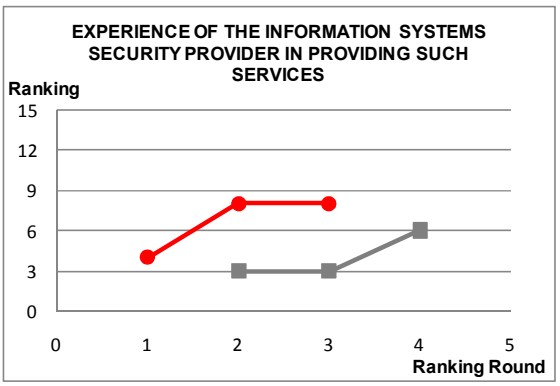


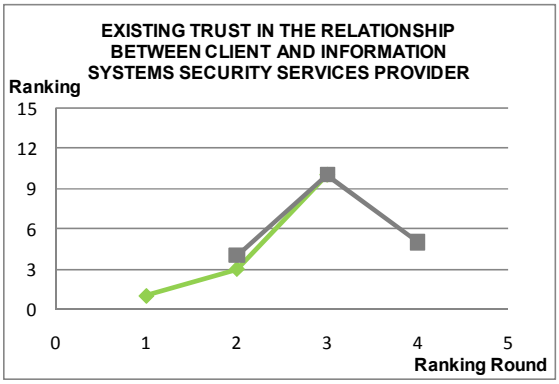
Figure C-4 – Round Answers from Participant [P5]

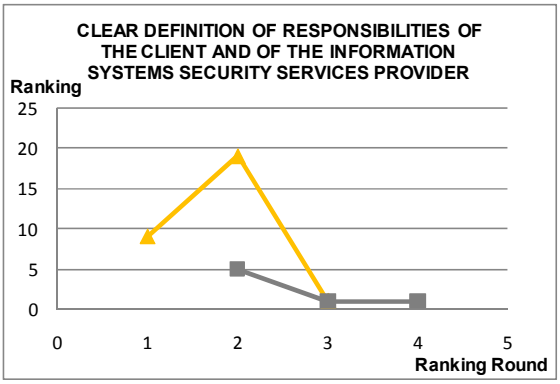












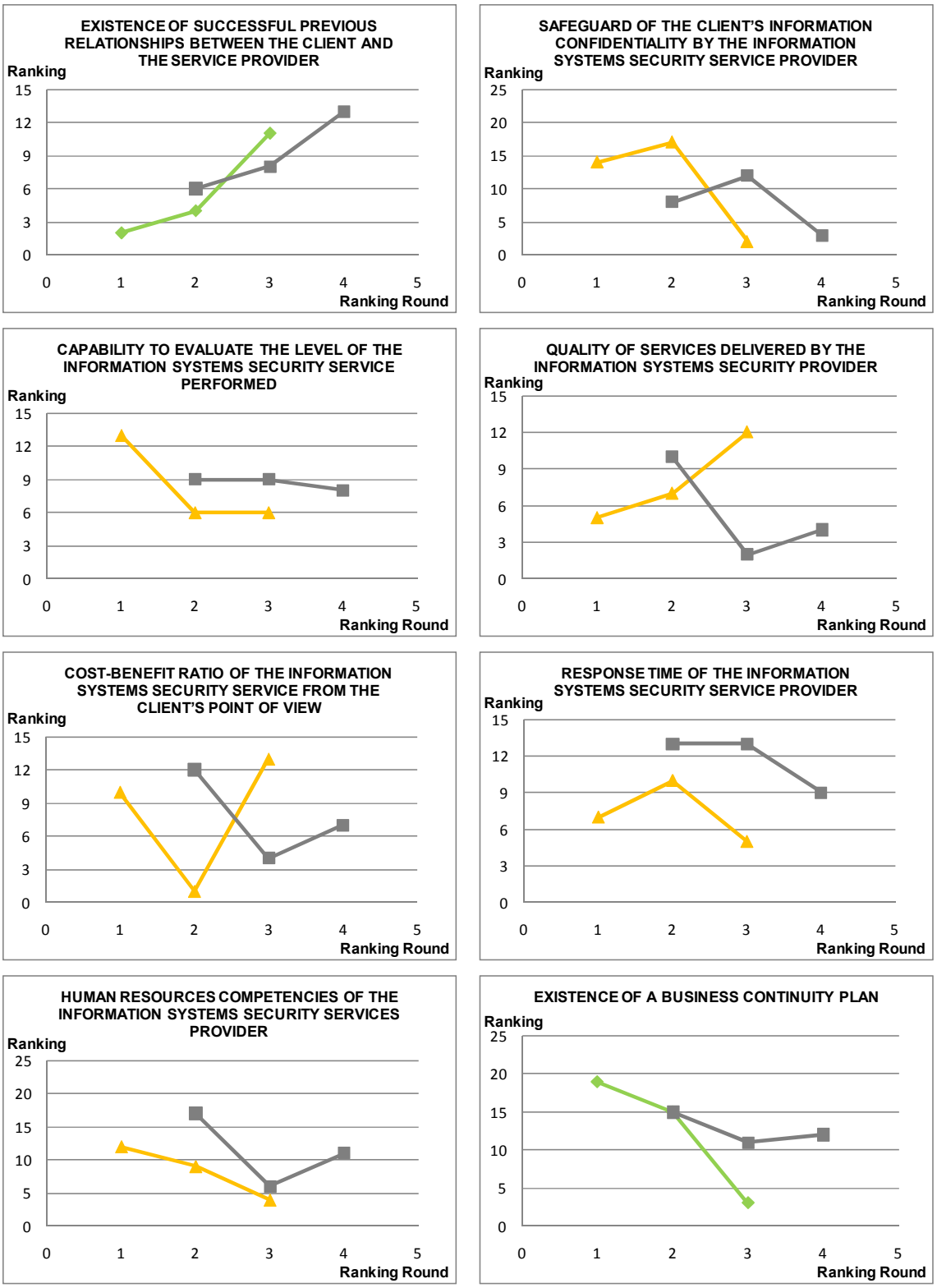
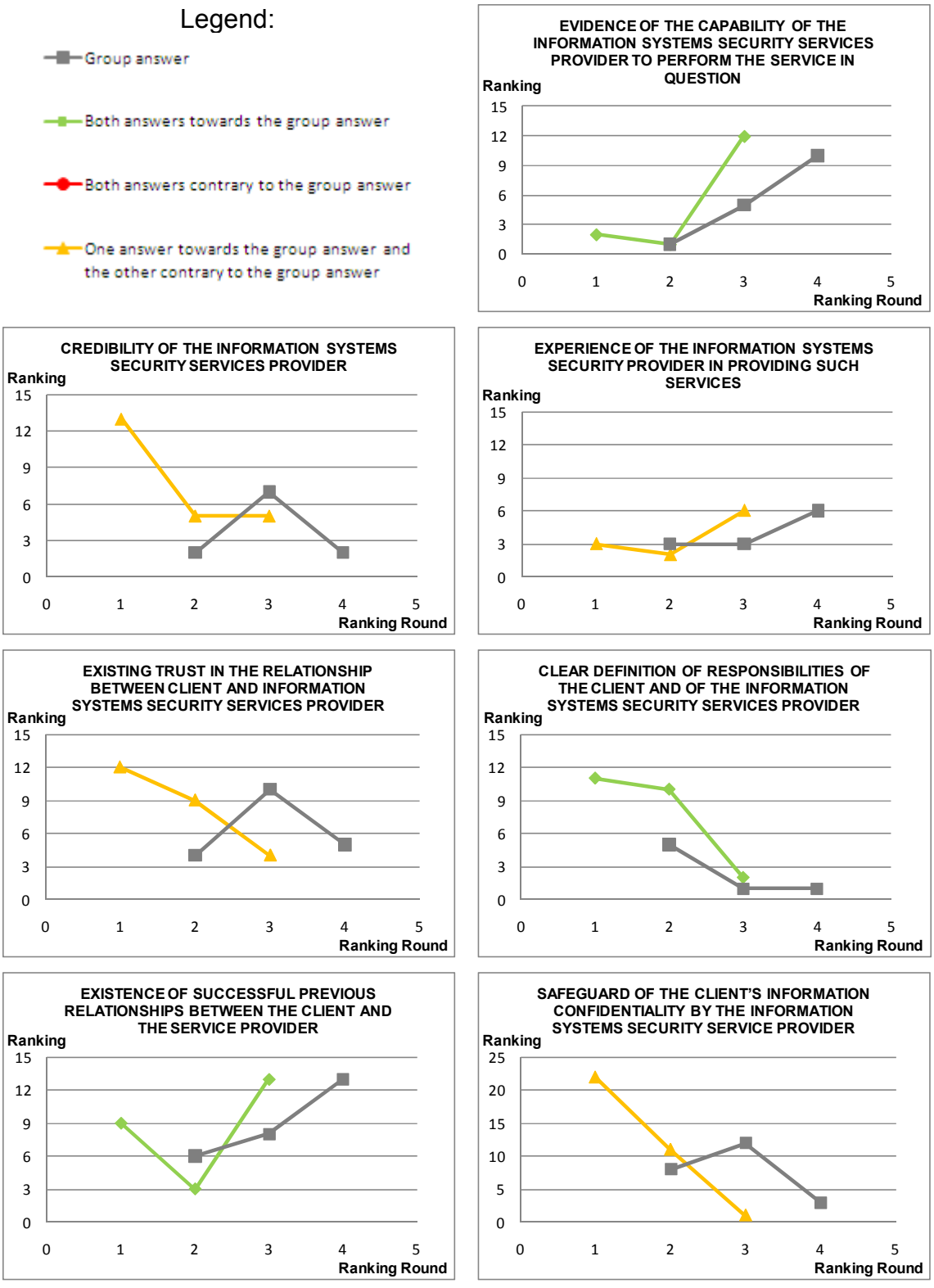


Figure C-5 – Round Answers from Participant [P6]


Legend:
Group answer
Both answers towards the group answer
Both answers contrary to the group answer
One answer towards the group answer and the other contrary to the group answer
EVIDENCE OF THE CAPABILITY OF THE INFORMATION SYSTEMS SECURITY SERVICES PROVIDER TO PERFORM THE SERVICE IN QUESTION
CREDIBILITY OF THE INFORMATION SYSTEMS SECURITY SERVICES PROVIDER
EXPERIENCE OF THE INFORMATION SYSTEMS SECURITY PROVIDER IN PROVIDING SUCH SERVICES
EXISTING TRUST IN THE RELATIONSHIP BETWEEN CLIENT AND INFORMATION SYSTEMS SECURITY SERVICES PROVIDER
CLEAR DEFINITION OF RESPONSIBILITIES OF THE CLIENT AND OF THE INFORMATION SYSTEMS SECURITY SERVICES PROVIDER
EXISTENCE OF SUCCESSFUL PREVIOUS RELATIONSHIPS BETWEEN THE CLIENT AND THE SERVICE PROVIDER
SAFEGUARD OF THE CLIENT'S INFORMATION CONFIDENTIALITY BY THE INFORMATION SYSTEMS SECURITY SERVICE PROVIDER
Ranking
Ranking Round

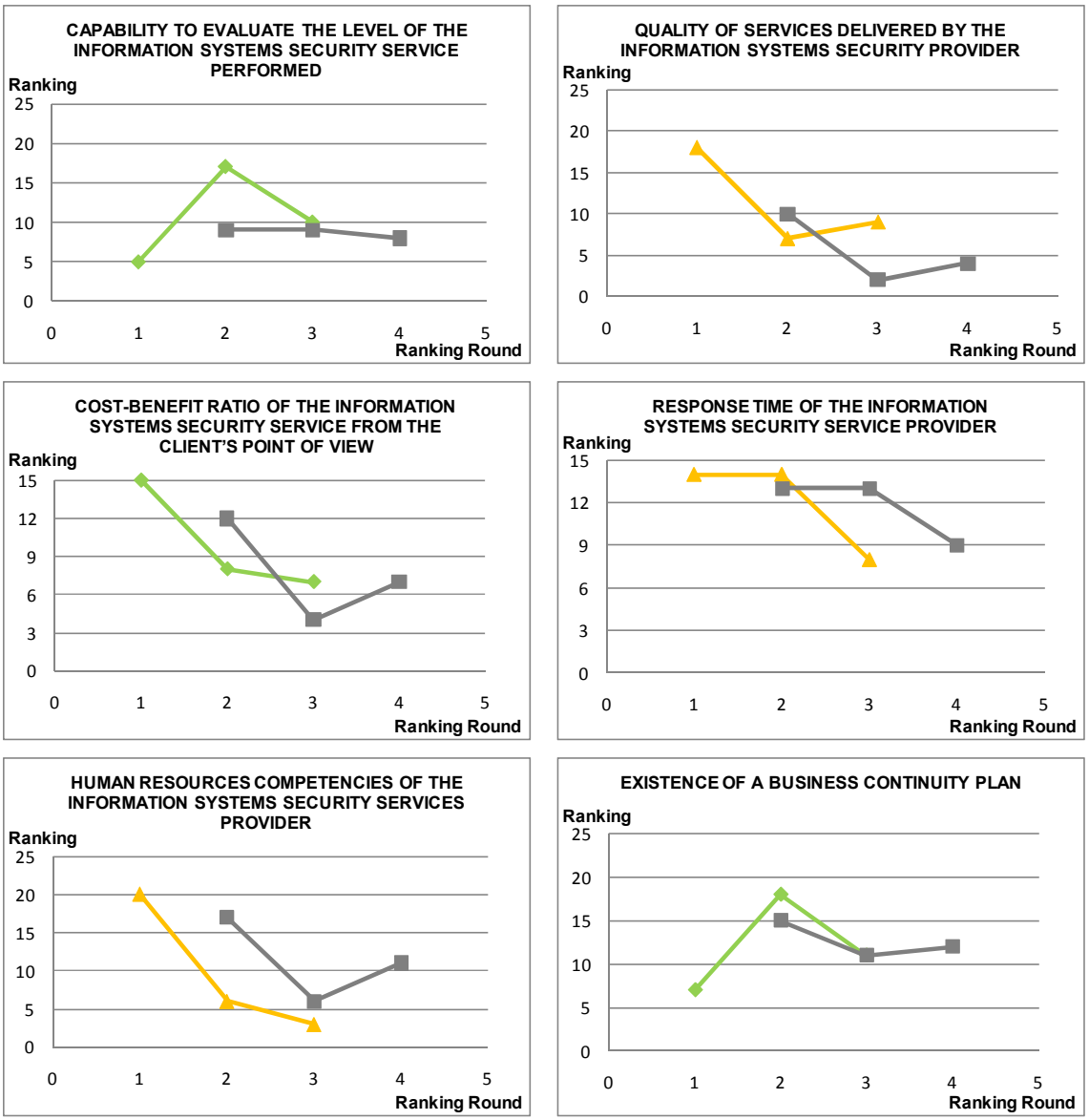
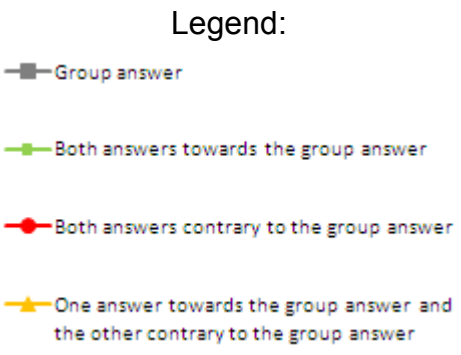
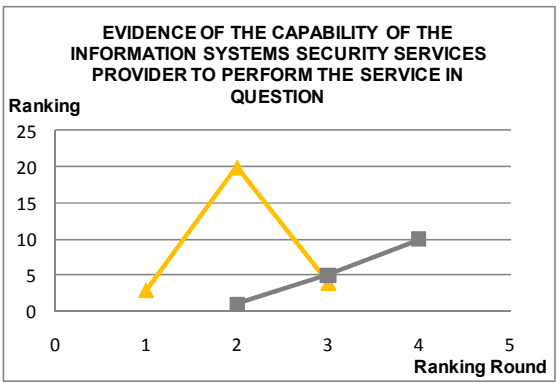
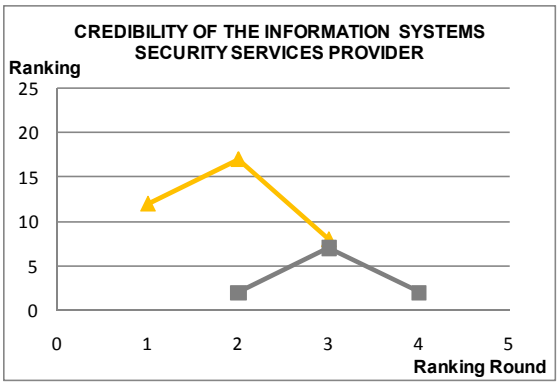
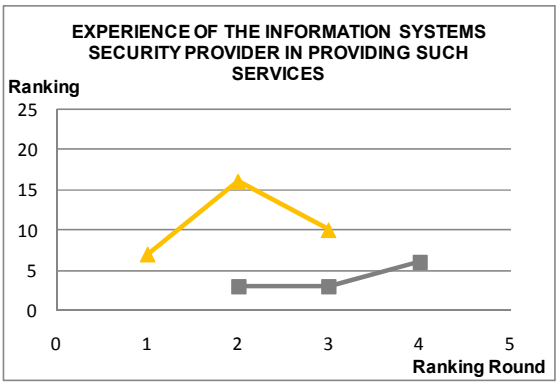


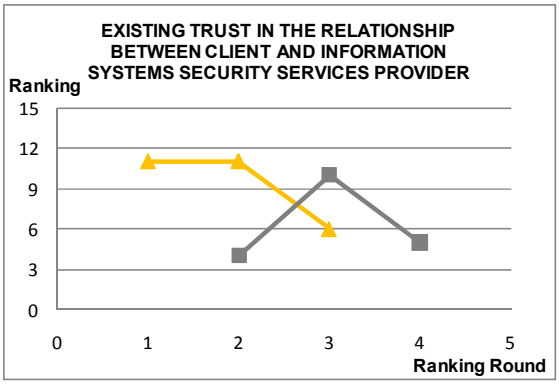
Figure C-6 – Round Answers from Participant [P7]

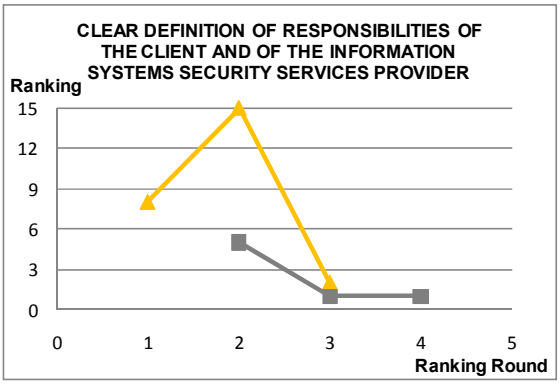


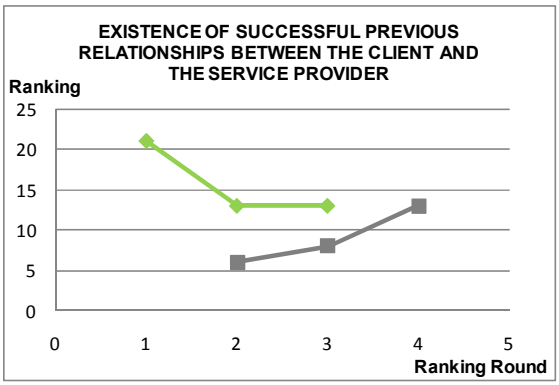


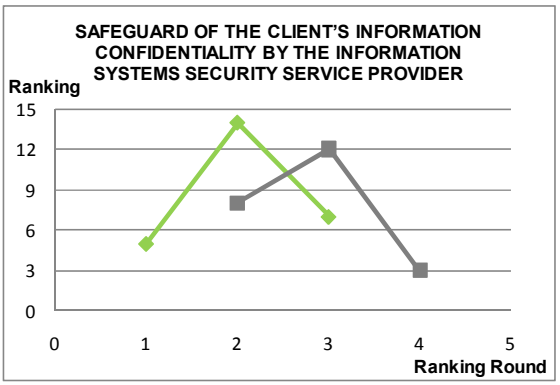

CREDIBILITY OF THE INFORMATION SYSTEMS SECURITY SERVICES PROVIDER
Ranking
25
20
15
10
5
0
0 1 2 3 4 5
Ranking Round

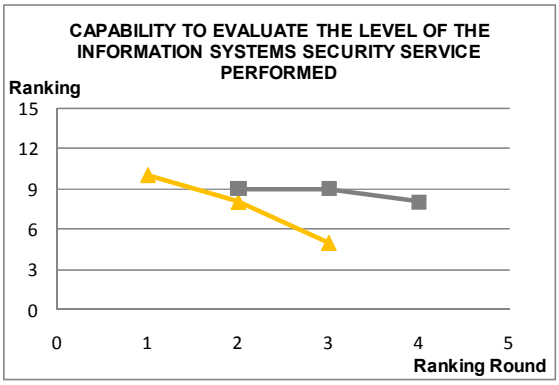

EXPERIENCE OF THE INFORMATION SYSTEMS SECURITY PROVIDER IN PROVIDING SUCH SERVICES
Ranking
25
20
15
10
5
0
0 1 2 3 4 5
Ranking Round

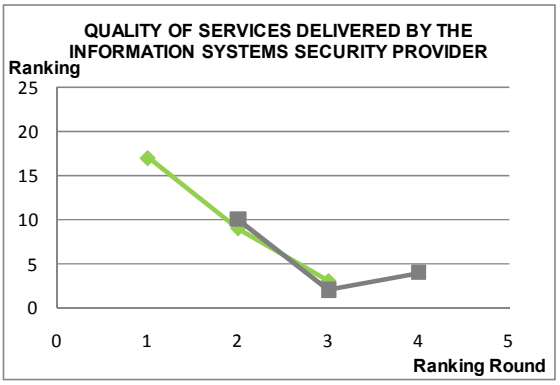

EXISTING TRUST IN THE RELATIONSHIP BETWEEN CLIENT AND INFORMATION SYSTEMS SECURITY SERVICES PROVIDER
Ranking
15
12
9
6
3
0
0 1 2 3 4 5
Ranking Round


CLEAR DEFINITION OF RESPONSIBILITIES OF THE CLIENT AND OF THE INFORMATION SYSTEMS SECURITY SERVICES PROVIDER
Ranking
15
12
9
6
3
0
0 1 2 3 4 5
Ranking Round


EXISTENCE OF SUCCESSFUL PREVIOUS RELATIONSHIPS BETWEEN THE CLIENT AND THE SERVICE PROVIDER
Ranking
25
20
15
10
5
0
0 1 2 3 4 5
Ranking Round


SAFEGUARD OF THE CLIENT'S INFORMATION CONFIDENTIALITY BY THE INFORMATION SYSTEMS SECURITY SERVICE PROVIDER
Ranking
15
12
9
6
3
0
0 1 2 3 4 5
Ranking Round


CAPABILITY TO EVALUATE THE LEVEL OF THE INFORMATION SYSTEMS SECURITY SERVICE PERFORMED
Ranking
15
12
9
6
3
0
0 1 2 3 4 5
Ranking Round


QUALITY OF SERVICES DELIVERED BY THE INFORMATION SYSTEMS SECURITY PROVIDER
Ranking
25
20
15
10
5
0
0 1 2 3 4 5
Ranking Round

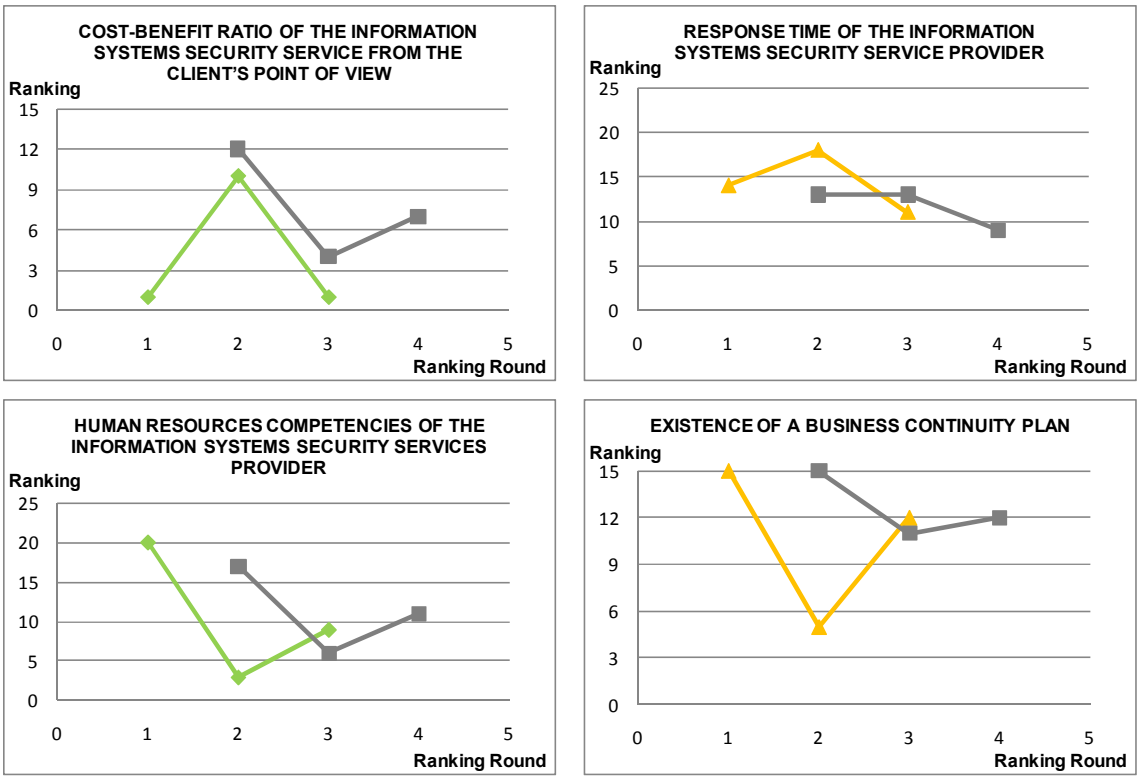
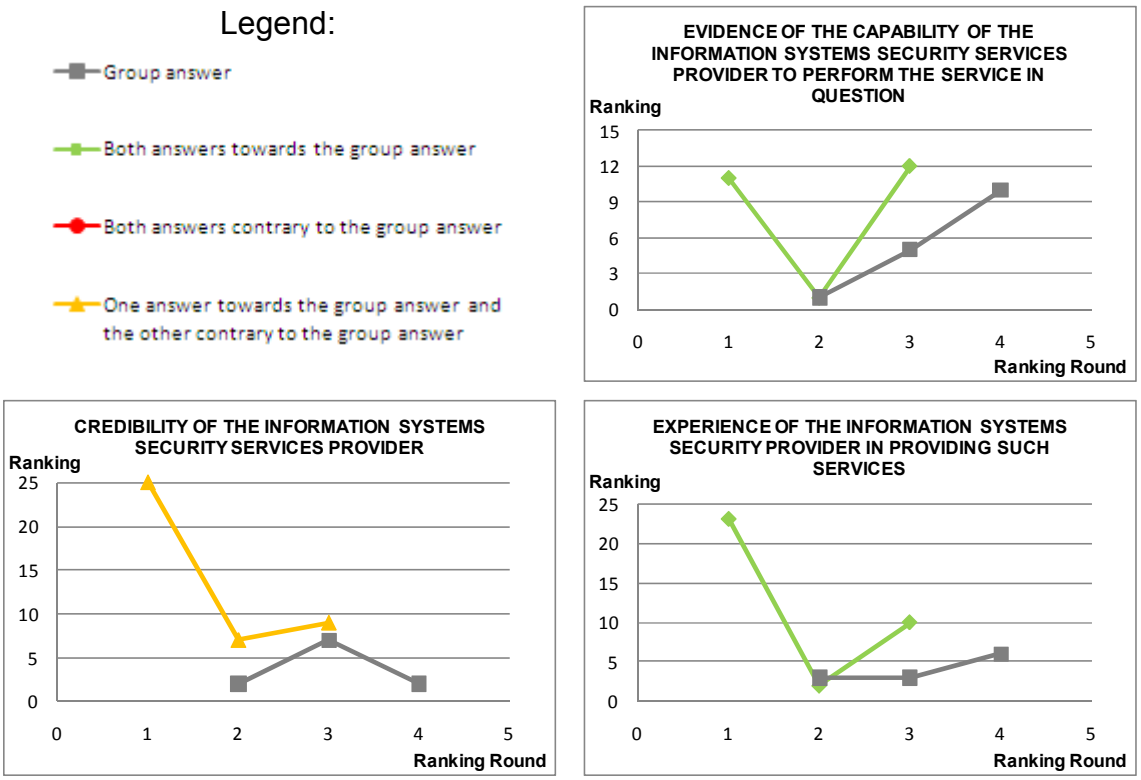
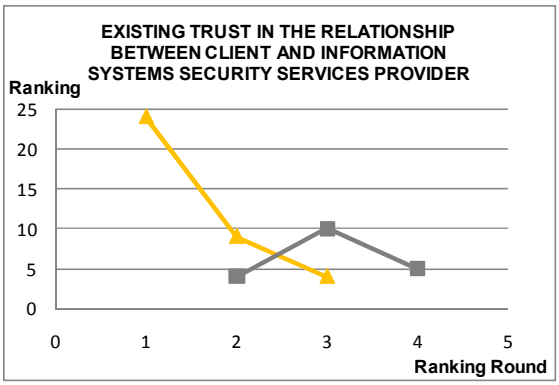
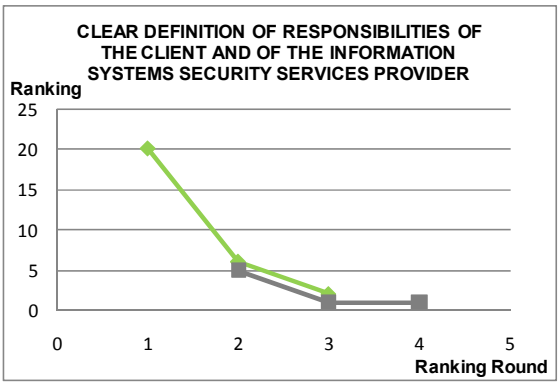
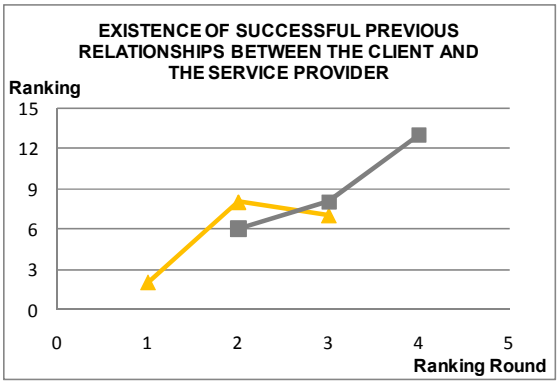


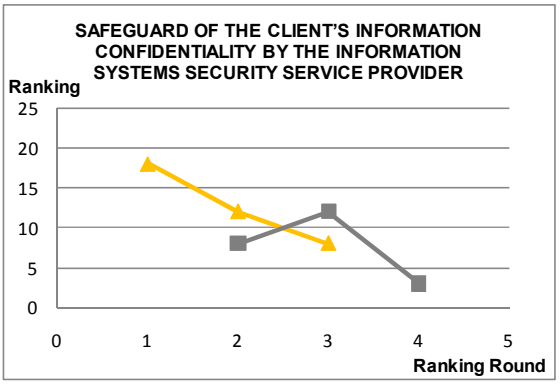
Figure C-7 – Round Answers from Participant [P8]

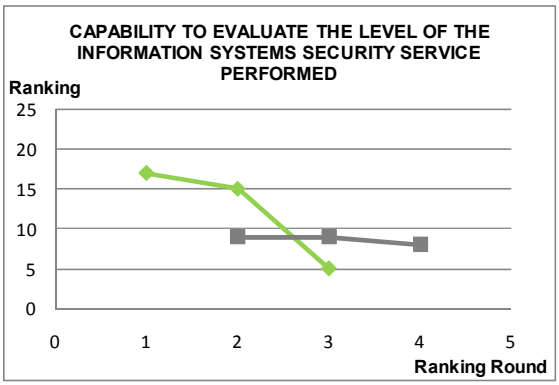


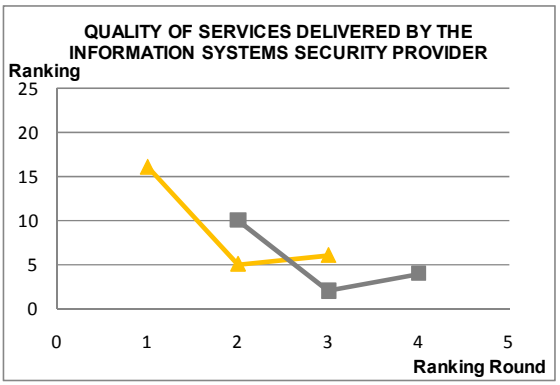

EXISTING TRUST IN THE RELATIONSHIP BETWEEN CLIENT AND INFORMATION SYSTEMS SECURITY SERVICES PROVIDER
Ranking
25
20
15
10
5
0
0 1 2 3 4 5
Ranking Round

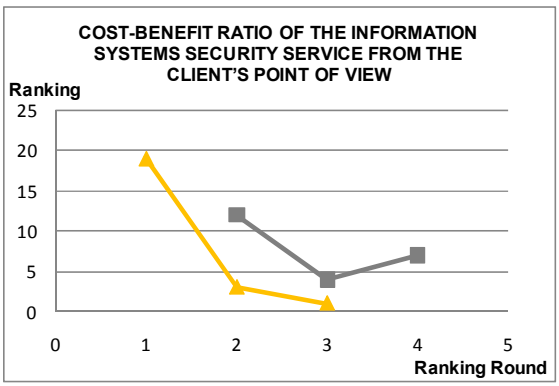

CLEAR DEFINITION OF RESPONSIBILITIES OF THE CLIENT AND OF THE INFORMATION SYSTEMS SECURITY SERVICES PROVIDER
Ranking
25
20
15
10
5
0
0 1 2 3 4 5
Ranking Round

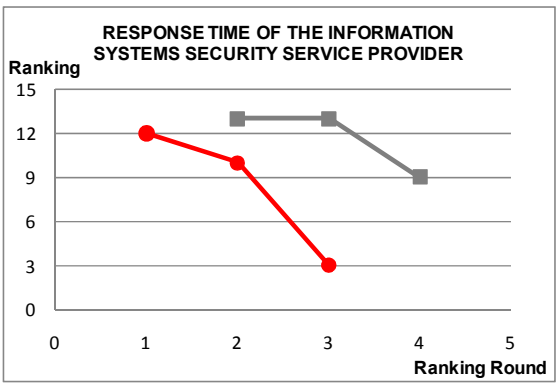

EXISTENCE OF SUCCESSFUL PREVIOUS RELATIONSHIPS BETWEEN THE CLIENT AND THE SERVICE PROVIDER
Ranking
15
12
9
6
3
0
0 1 2 3 4 5
Ranking Round


SAFEGUARD OF THE CLIENT'S INFORMATION CONFIDENTIALITY BY THE INFORMATION SYSTEMS SECURITY SERVICE PROVIDER
Ranking
25
20
15
10
5
0
0 1 2 3 4 5
Ranking Round


CAPABILITY TO EVALUATE THE LEVEL OF THE INFORMATION SYSTEMS SECURITY SERVICE PERFORMED
Ranking
25
20
15
10
5
0
0 1 2 3 4 5
Ranking Round


QUALITY OF SERVICES DELIVERED BY THE INFORMATION SYSTEMS SECURITY PROVIDER
Ranking
25
20
15
10
5
0
0 1 2 3 4 5
Ranking Round


COST-BENEFIT RATIO OF THE INFORMATION SYSTEMS SECURITY SERVICE FROM THE CLIENT'S POINT OF VIEW
Ranking
25
20
15
10
5
0
0 1 2 3 4 5
Ranking Round


RESPONSE TIME OF THE INFORMATION SYSTEMS SECURITY SERVICE PROVIDER
Ranking
15
12
9
6
3
0
0 1 2 3 4 5
Ranking Round

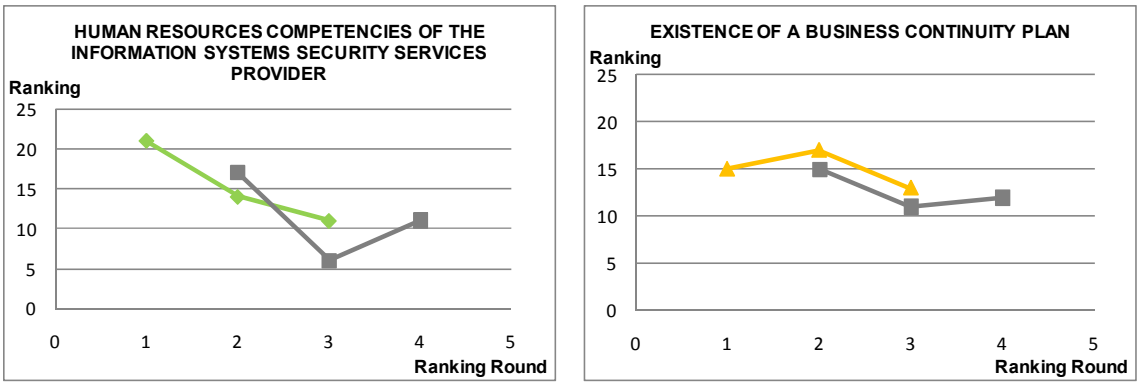
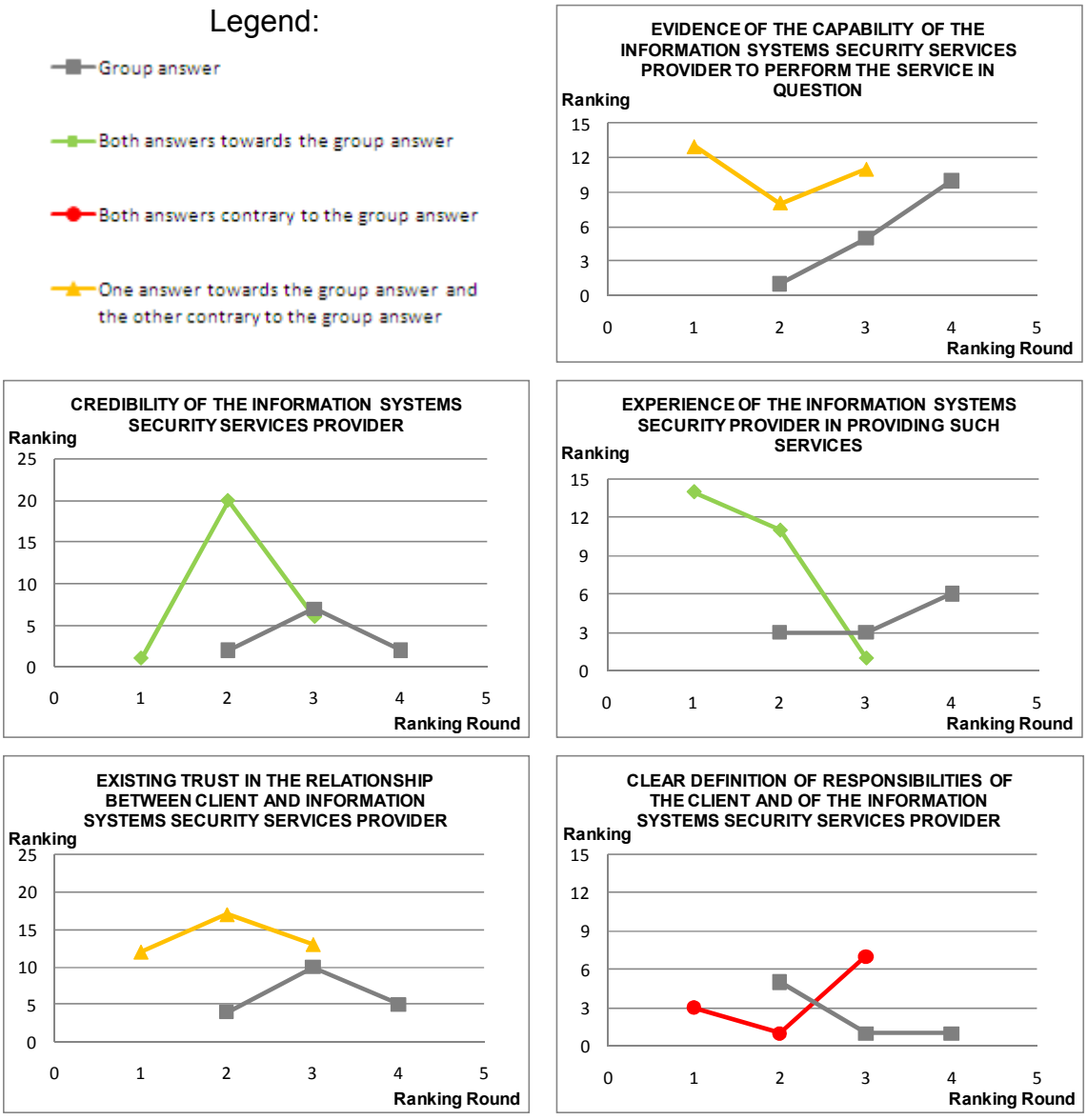


Figure C-8 – Round Answers from Participant [P9]



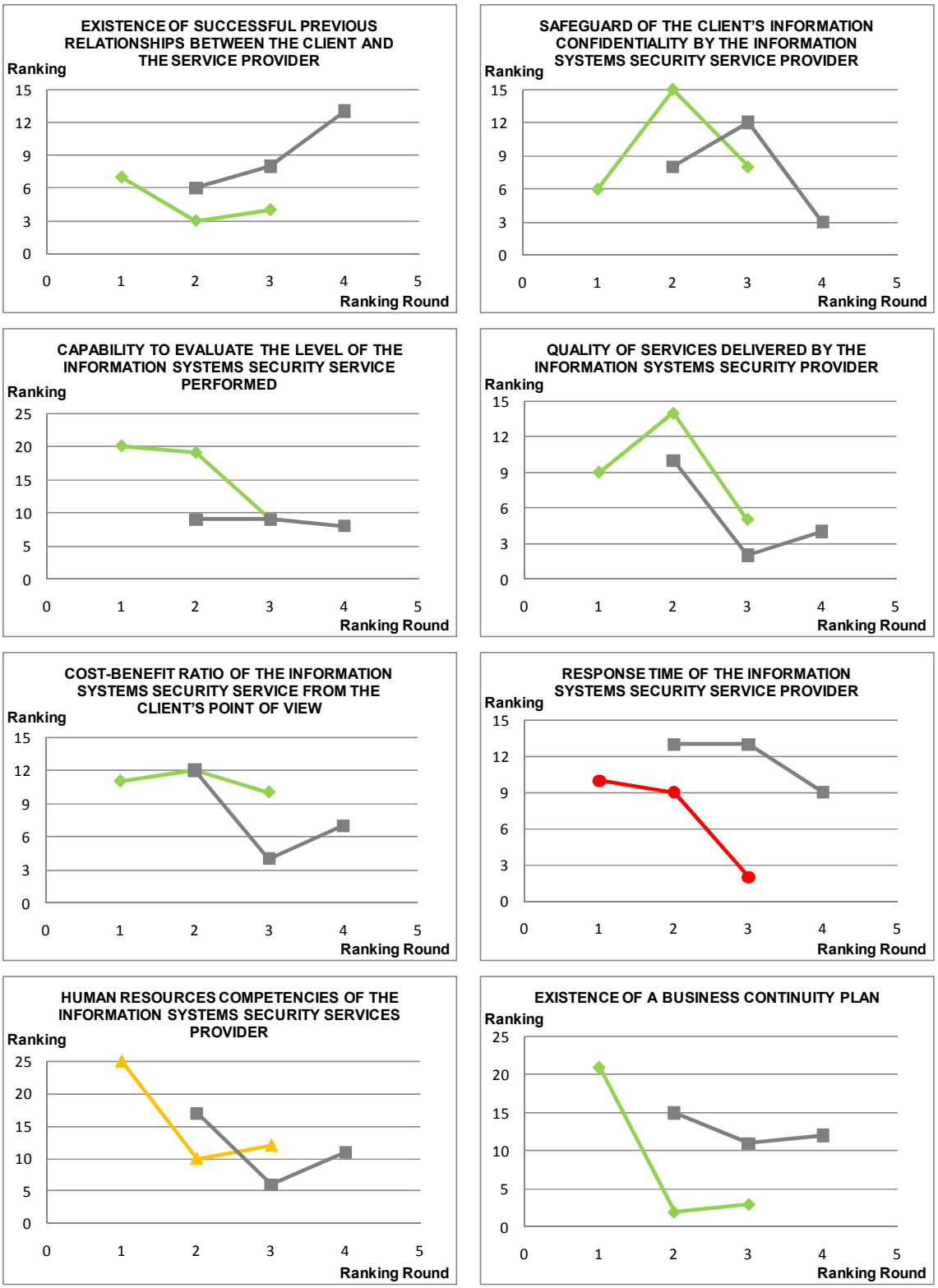
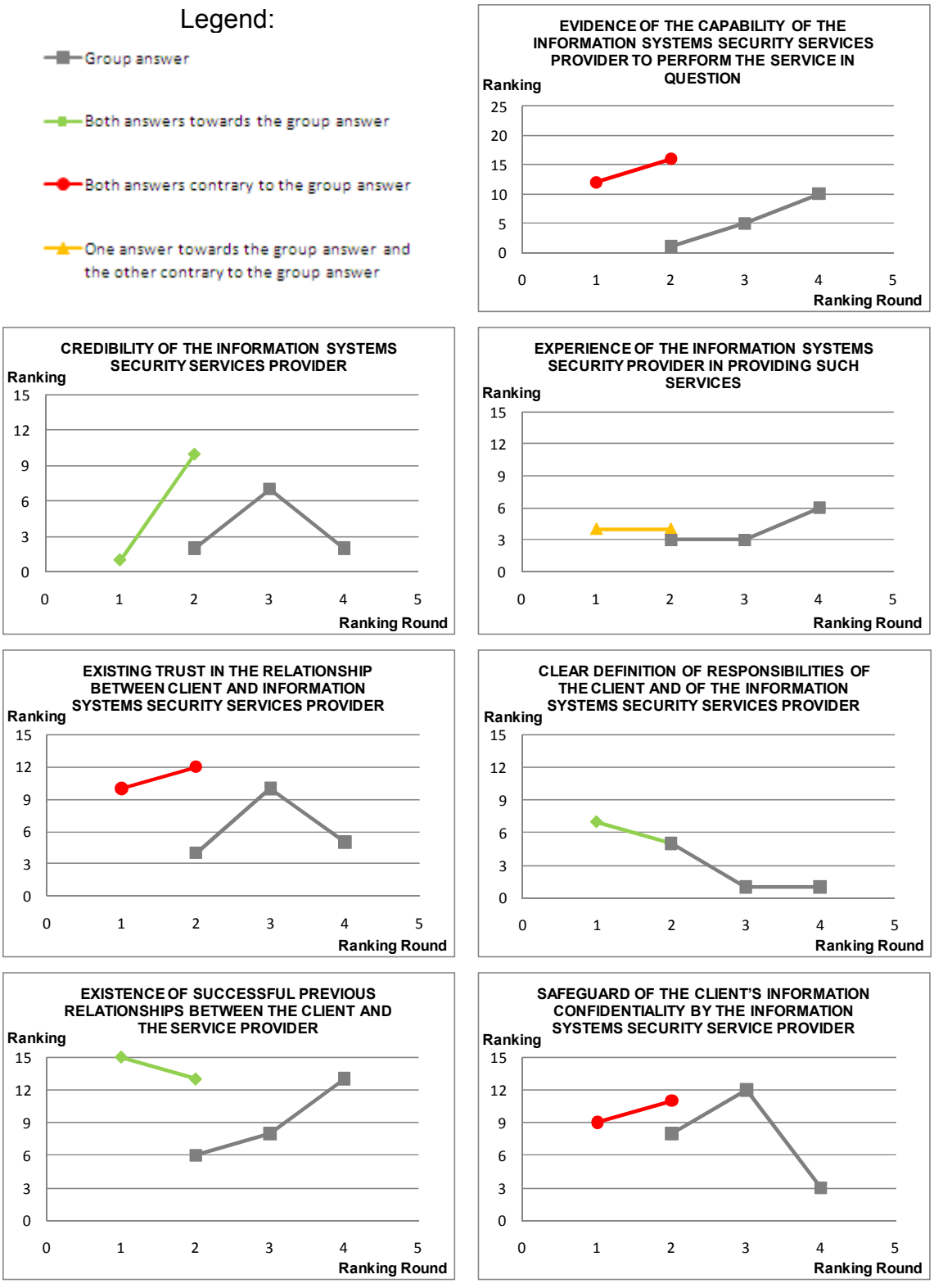


Figure C-9 – Round Answers from Participant [P10]


Legend:
Group answer
Both answers towards the group answer
Both answers contrary to the group answer
One answer towards the group answer and the other contrary to the group answer
EVIDENCE OF THE CAPABILITY OF THE INFORMATION SYSTEMS SECURITY SERVICES PROVIDER TO PERFORM THE SERVICE IN QUESTION
CREDIBILITY OF THE INFORMATION SYSTEMS SECURITY SERVICES PROVIDER
EXPERIENCE OF THE INFORMATION SYSTEMS SECURITY PROVIDER IN PROVIDING SUCH SERVICES
EXISTING TRUST IN THE RELATIONSHIP BETWEEN CLIENT AND INFORMATION SYSTEMS SECURITY SERVICES PROVIDER
CLEAR DEFINITION OF RESPONSIBILITIES OF THE CLIENT AND OF THE INFORMATION SYSTEMS SECURITY SERVICES PROVIDER
EXISTENCE OF SUCCESSFUL PREVIOUS RELATIONSHIPS BETWEEN THE CLIENT AND THE SERVICE PROVIDER
SAFEGUARD OF THE CLIENT'S INFORMATION CONFIDENTIALITY BY THE INFORMATION SYSTEMS SECURITY SERVICE PROVIDER
Ranking
Ranking Round

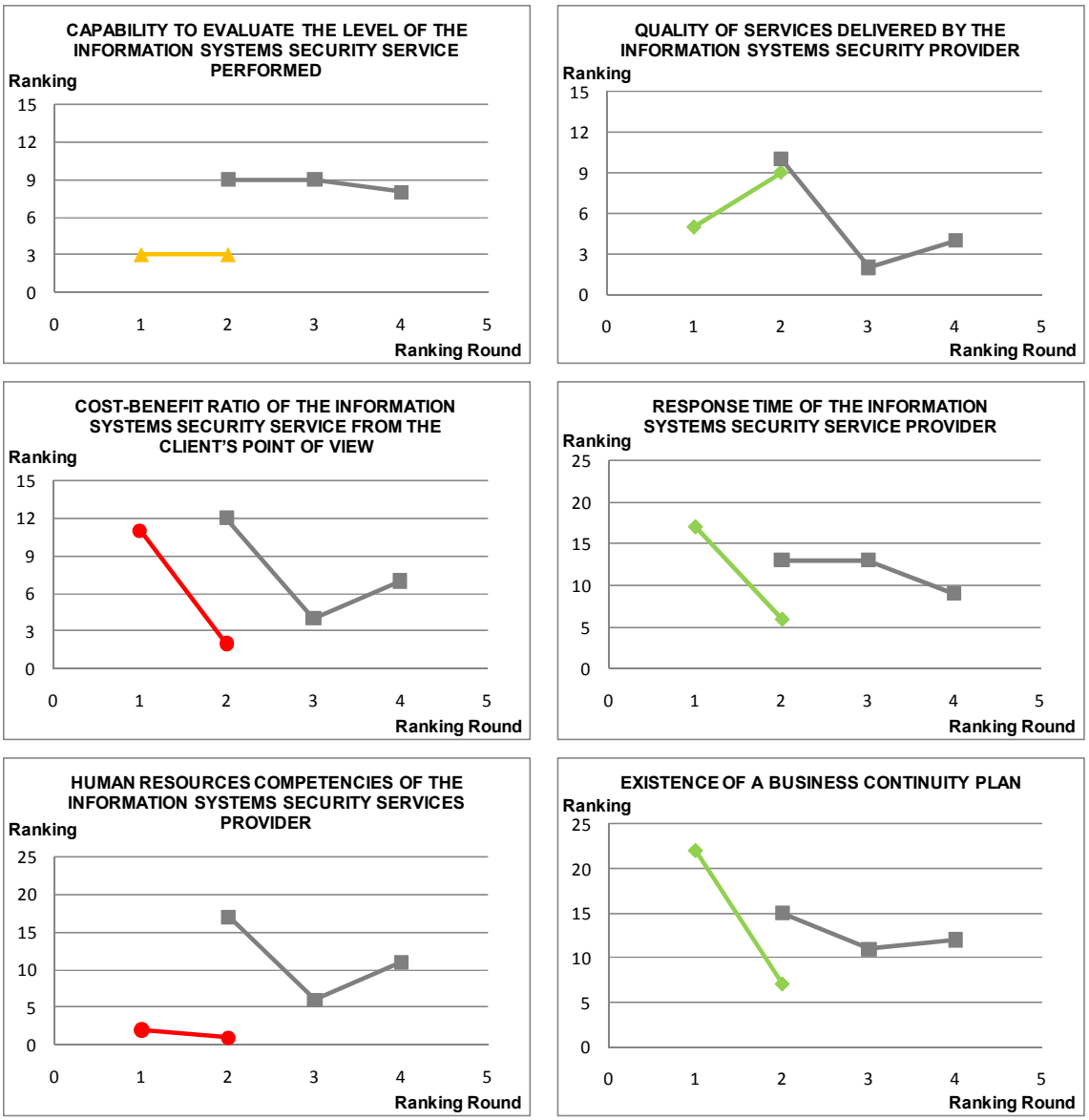
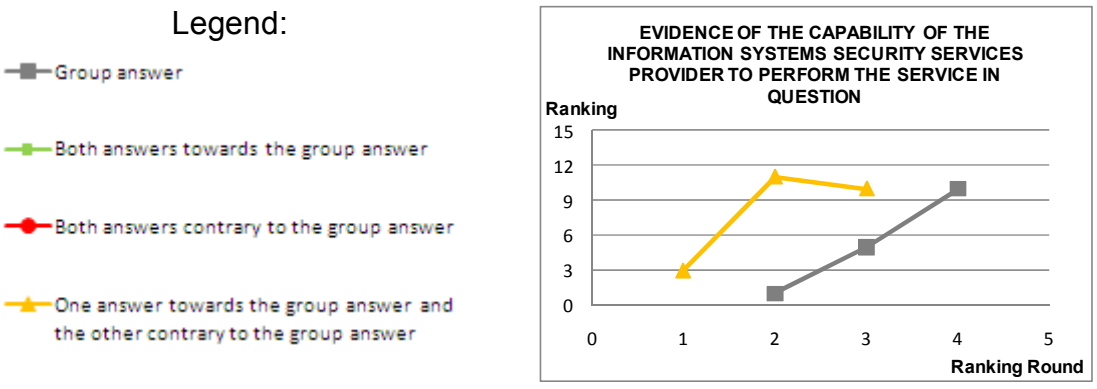
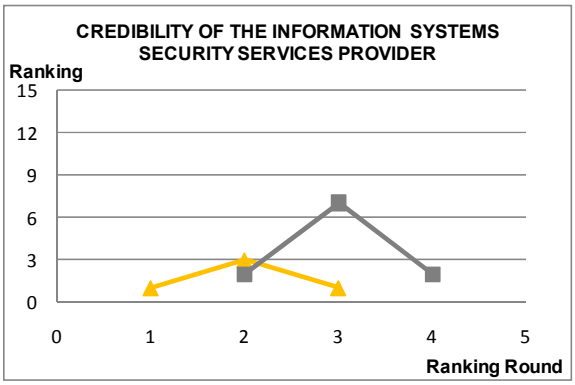
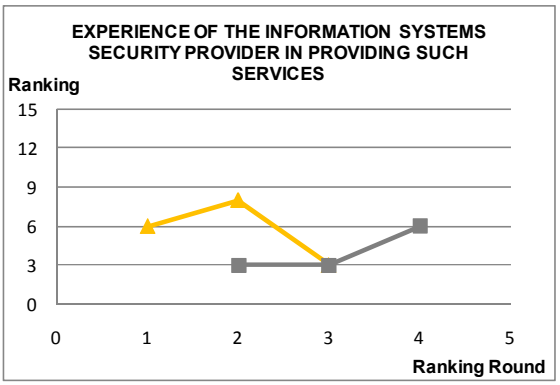
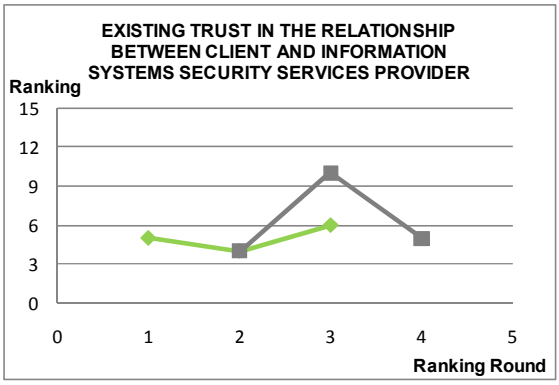


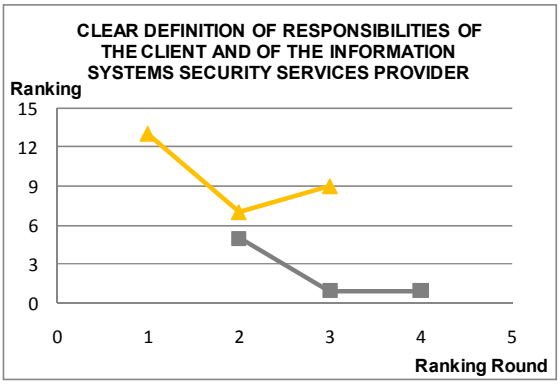
Figure C-10 – Round Answers from Participant [P13]

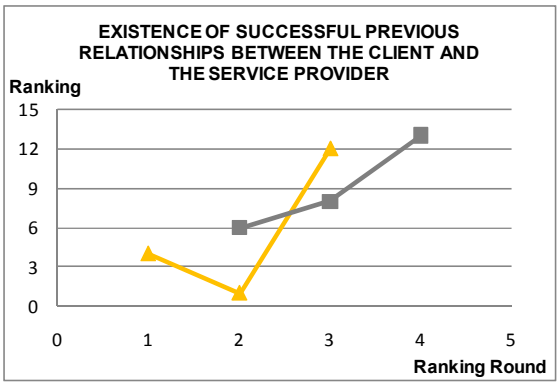


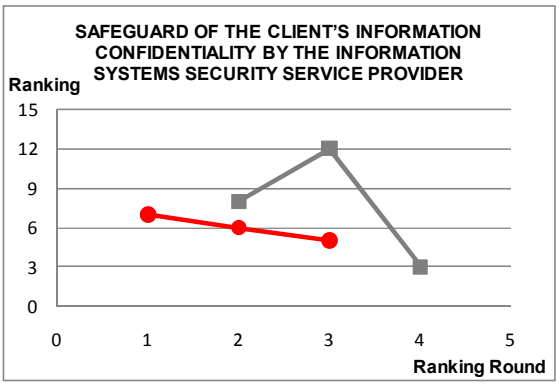

CREDIBILITY OF THE INFORMATION SYSTEMS SECURITY SERVICES PROVIDER
Ranking
15
12
9
6
3
0
0 1 2 3 4 5
Ranking Round

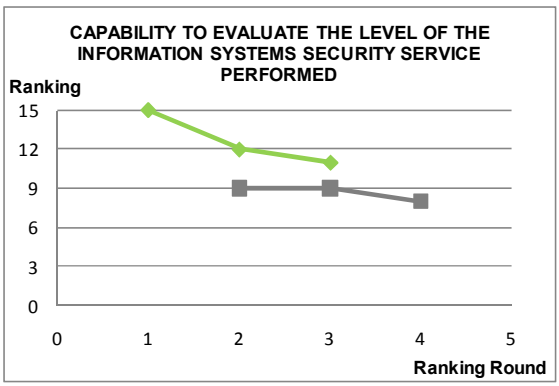

EXPERIENCE OF THE INFORMATION SYSTEMS SECURITY PROVIDER IN PROVIDING SUCH SERVICES
Ranking
15
12
9
6
3
0
0 1 2 3 4 5
Ranking Round

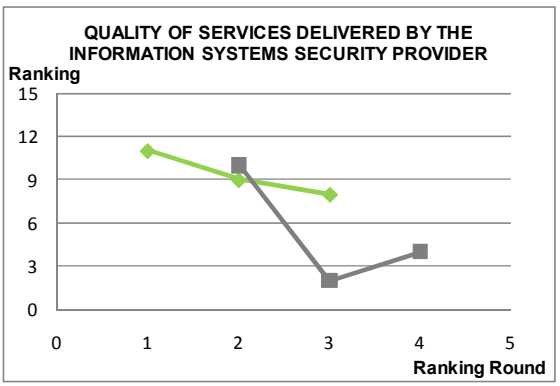

EXISTING TRUST IN THE RELATIONSHIP BETWEEN CLIENT AND INFORMATION SYSTEMS SECURITY SERVICES PROVIDER
Ranking
15
12
9
6
3
0
0 1 2 3 4 5
Ranking Round


CLEAR DEFINITION OF RESPONSIBILITIES OF THE CLIENT AND OF THE INFORMATION SYSTEMS SECURITY SERVICES PROVIDER
Ranking
15
12
9
6
3
0
0 1 2 3 4 5
Ranking Round


EXISTENCE OF SUCCESSFUL PREVIOUS RELATIONSHIPS BETWEEN THE CLIENT AND THE SERVICE PROVIDER
Ranking
15
12
9
6
3
0
0 1 2 3 4 5
Ranking Round


SAFEGUARD OF THE CLIENT'S INFORMATION CONFIDENTIALITY BY THE INFORMATION SYSTEMS SECURITY SERVICE PROVIDER
Ranking
15
12
9
6
3
0
0 1 2 3 4 5
Ranking Round


CAPABILITY TO EVALUATE THE LEVEL OF THE INFORMATION SYSTEMS SECURITY SERVICE PERFORMED
Ranking
15
12
9
6
3
0
0 1 2 3 4 5
Ranking Round


QUALITY OF SERVICES DELIVERED BY THE INFORMATION SYSTEMS SECURITY PROVIDER
Ranking
15
12
9
6
3
0
0 1 2 3 4 5
Ranking Round

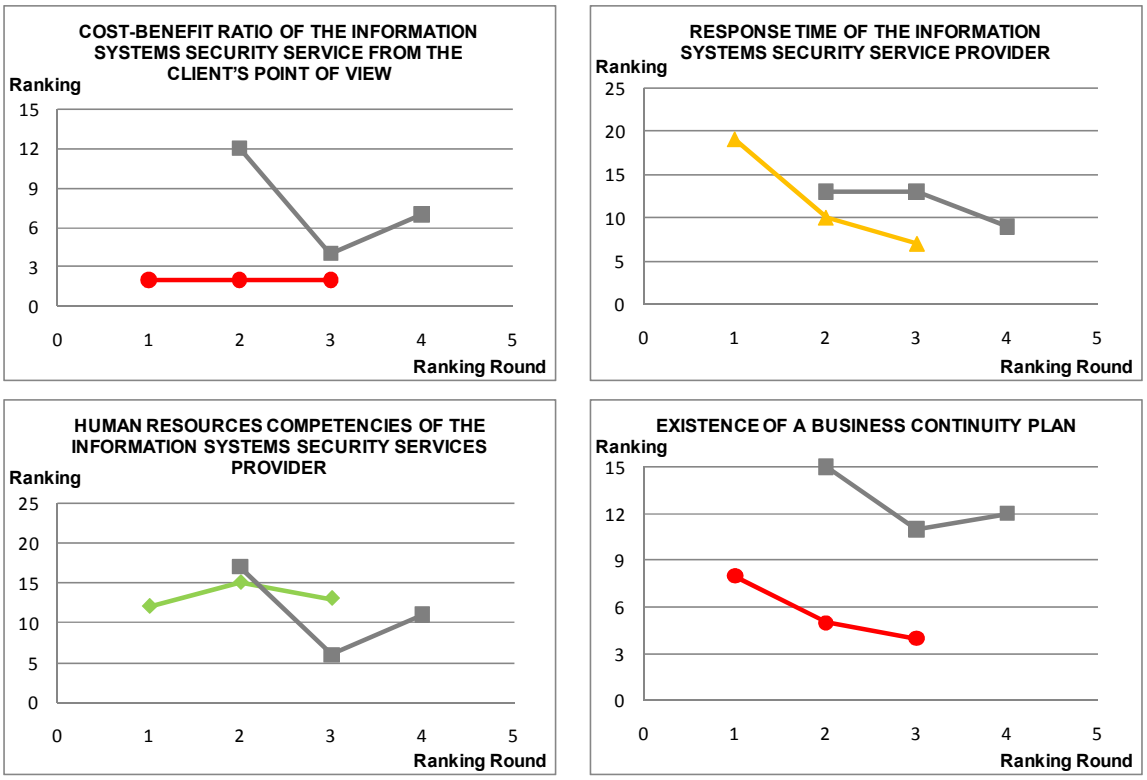


Figure C-11 – Round Answers from Participant [P14]