A FRAMEWORK TO EVALUATE USABLE SECURITY IN ONLINE SOCIAL NETWORKING

By

Alexandros Yeratziotis

2011

A FRAMEWORK TO EVALUATE USABLE SECURITY IN ONLINE SOCIAL NETWORKING

By

Alexandros Yeratziotis

Thesis

submitted in fulfilment of the requirements for the degree

Philosophiae Doctor

in

Information Technology

in the

Faculty of Engineering, the Built Environment and

Information Technology

of the

Nelson Mandela Metropolitan University

Promoter: **Professor Darelle van Greunen**

Co-Promoter: **Professor Dalenca Pottas**

December 2011

DECLARATION

I, *Alexandros Yeratziotis s20323238*, hereby declare that the *thesis* for *Philosophiae Doctor: Information Technology* is my own work and that it has not previously been submitted for assessment or completion of any postgraduate qualification to another University or for another qualification.

Alexandros Yeratziotis

Official use:

In accordance with Rule G4.6.3,

4.6.3 A treatise/dissertation/thesis must be accompanied by a written declaration on the part of the candidate to the effect that it is his/her own work and that it has not previously been submitted for assessment to another University or for another qualification. However, material from publications by the candidate may be embodied in a treatise/dissertation/thesis.

ACKNOWLEDGMENTS

I thank the Lord for infinite blessings and for granting me the health and strength to persevere.

My sincere gratitude goes to:

My promoter, **Prof. Darelle van Greunen**: Thank you for being part of this lengthy journey that essentially started in 2006 after one of your classes I attended in my B-Tech year. We have come a long way since then and I am privileged to have shared this journey with you at the helm. Your knowledge and contribution to the field is massive. I have learnt a lot from you over the years but, besides that, what I appreciate the most is that you have always stood by me as a close friend as well and not just as a supervisor. Whenever I needed help or an opportunity you always provided it and for this I thank you the most.

My co-promoter, **Prof. Dalenca Pottas**: Thank you for being part of this lengthy journey as well. Your expertise was fundamental to the success of this research study and your sustained and indispensable advice, guidance and encouragement are much appreciated. I have enjoyed sharing this experience with you and it has been a privilege to learn from you.

The financial assistance from **Research Capacity Development** (RCD) at the Nelson Mandela Metropolitan University (NMMU), the **German Academic Exchange Service** and the **National Research Foundation** (DAAD/NRF) of South Africa and the **South Africa – Finland Knowledge Partnership on ICT** (SAFIPA): Thank you for the continual financial assistance that was provided to me during the course of my postgraduate studies and for the six-month exchange visit to Aalto University in Finland.

The editor, **Alexa Barnby**: Thank you for the dedicated hours you spent editing this document to ensure its professional and concise presentation.

The six participants and four experts: Thank you for taking the time out of your busy schedules to contribute in my research study and to provide me with the valuable feedback that you have.

My family, **Elias**, **Eleni**, **George** and **Theofilia**: Thank you for your unconditional love, sacrifice, devoted support, understanding and encouragement. Elias, you are a great man and I will always look up to you and follow your examples.

To the families, **Ioannou**, **Storm**, **Rau** and **Gregoriou**: Thank you for your support and for always making me feel welcome in your homes and as a member of your families.

My brother, **Greg**: Thanks for just being you; always an example. Please, never change because you are special. Your strength and will is unmatched. You will always be a teacher without books and I will always remain your student.

My closest friends, **Andreas G.**, **Andreas I.**, **Andreas Y.**, **Antonis**, **Demetris**, **George**, **Liezel**, **Marios, Nicholas** and **Vasilis**: Thank you for your friendship and for positively influencing my life.

My fellow postgraduate students in the lab J113: Thank you for your help and support. We have spent many hours together over the past few years and have always assisted one other throughout our journey. Good luck with the rest of yours. Be strong and continue working as you do and you will all prevail.

ABSTRACT

It is commonly held in the literature that users find security and privacy difficult to comprehend. It is also acknowledged that most end-user applications and websites have built-in security and privacy features. Users are expected to interact with these in order to protect their personal information. However, security is generally a secondary goal for users. Considering the complexity associated with security in combination with the notion that it is not users' primary task, it makes sense that users tend to ignore their security responsibilities. As a result, they make poor security-related decisions and, consequently, their personal information is at risk. Usable Security is the field that investigates these types of issue, focusing on the design of security and privacy features that are usable. In order to understand and appreciate the complexities that exist in the field of Usable Security, the research fields of Human-Computer Interaction and Information Security should be examined. Accordingly, the Information Security field is concerned with all aspects pertaining to the security and privacy of information, while the field of Human-Computer Interaction is concerned with the design, evaluation and implementation of interactive computing systems for human use.

This research delivers a framework to evaluate Usable Security in online social networks. In this study, online social networks that are particular to the health domain were used as a case study and contributed to the development of a framework consisting of three components: a process, a validation tool and a Usable Security heuristic evaluation. There is no existing qualitative process that describes how one would develop and validate a heuristic evaluation. In this regard a heuristic evaluation is a usability inspection method that is used to evaluate the design of an interface for any usability violations in the field of Human-Computer Interaction. Therefore, firstly, a new process and a validation tool were required to be developed. Once this had been achieved, the process could then be followed to develop a new heuristic evaluation that is specific to Usable Security. In order to assess the validity of a new heuristic evaluation a validation tool is used. The development of tools that can improve the design of security and privacy features on end-user applications and websites in terms of their usability is critical, as this will ensure that the intended users experience them as usable and can utilise them effectively. The framework for evaluating Usable Security contributes to this objective in the context of online social networks.

Keywords: User experience, usable security, heuristic evaluation, online social networks

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 6: CASE STUDY - ONLINE HEALTH SOCIAL NETWORKS 152

CHAPTER 7: RESULTS AND ANALYSIS FROM VALIDATION TOOL.......................185

CHAPTER 8: APPLICABILITY OF THE USABLE SECURITY FRAMEWORK 226

LIST OF ABBREVIATIONS

Abbreviations	Term in Full
COBIT	Control Objectives for Information and related Technology
CSF	Common Security Framework
FIP	Codes of Fair Information Practice
FIPS	Fair Information Practices
FTC	Fair Information Practices in the Electronic Marketplace
FUE	Formative Usability Evaluation
GAPP	Generally Accepted Privacy Principles
GLBA	Gramm-Leach-Bliley Act
GUP	Graphical presentation of User Profile
HCD	Human-Centred Design
HCI	Human-Computer Interaction
HCI-S	Human Computer Interaction applied in the area of computer Security
HE	Heuristic Evaluation
HIPAA	Health Insurance Portability and Accountability Act
HITRUST	Health Information Trust Alliance
IA	Information Architecture
ICT	Information and Communication Technologies
ID	Interaction Design
InfoSec	Information Security
ISO	International Organization for Standardization
ISTPA	International Security, Trust and Privacy Alliance
IT	Information Technology
MS	Microsoft
NIST	National Institute of Standards and Technology
OECD	Organization for Economic Cooperation and Development
OHSN	Online Health Social Network
PHI	Personal Health Information
PHR	Personal Health Record
PIPEDA	Canada Personal Information Protection and Electronic Documents Act
PKI	Public Key Infrastructure
PMM	Privacy Maturity Model
SAD	Specific Application Domain
SCD	System-Centred Design
UCD	User-Centred Design
UCSD	User-Centred System Design
UED	User Environment Design
UI	User Interface
UIM	Usability Inspection Method
USec	Usable Security
UX	User Experience

AUTHOR PUBLICATIONS

The following publications stemmed directly from the work in this thesis:

1. Yeratziotis, A., Pottas, D. & van Greunen, D. (2011). Recommendations for Usable Security in Online Health Social Networks. In Proceedings of the joint conference of the 2011 6th International Conference on Pervasive Computing and Application (ICPCA) and the 2011 3rd International Symposium of Web Society (SWS), 26-28 October 2011, Port Elizabeth, South Africa.
2. Yeratziotis, A., Pottas, D. & van Greunen, D. (2011). A Three-Phase Process to Develop Heuristics, 13th ZA-WWW conference, 14–16 September 2011, Johannesburg.
3. Yeratziotis, A., Sannemann, C., Viitanen, J. & Nieminen, M. (2011). Analysis of Emergent Use for Wellbeing Service Innovation. Design, User Experience, and Usability, Pt I, HCII 2011, LNCS 6769, pp. 332–341, 2011. Springer-Verlag Berlin Heidelberg 2011.
4. Yeratziotis, A., Pottas, D. & van Greunen, D. (2012). A usable security heuristic evaluation for the online health social networking paradigm. International Journal of Human-Computer Interaction, vol. 29(3).

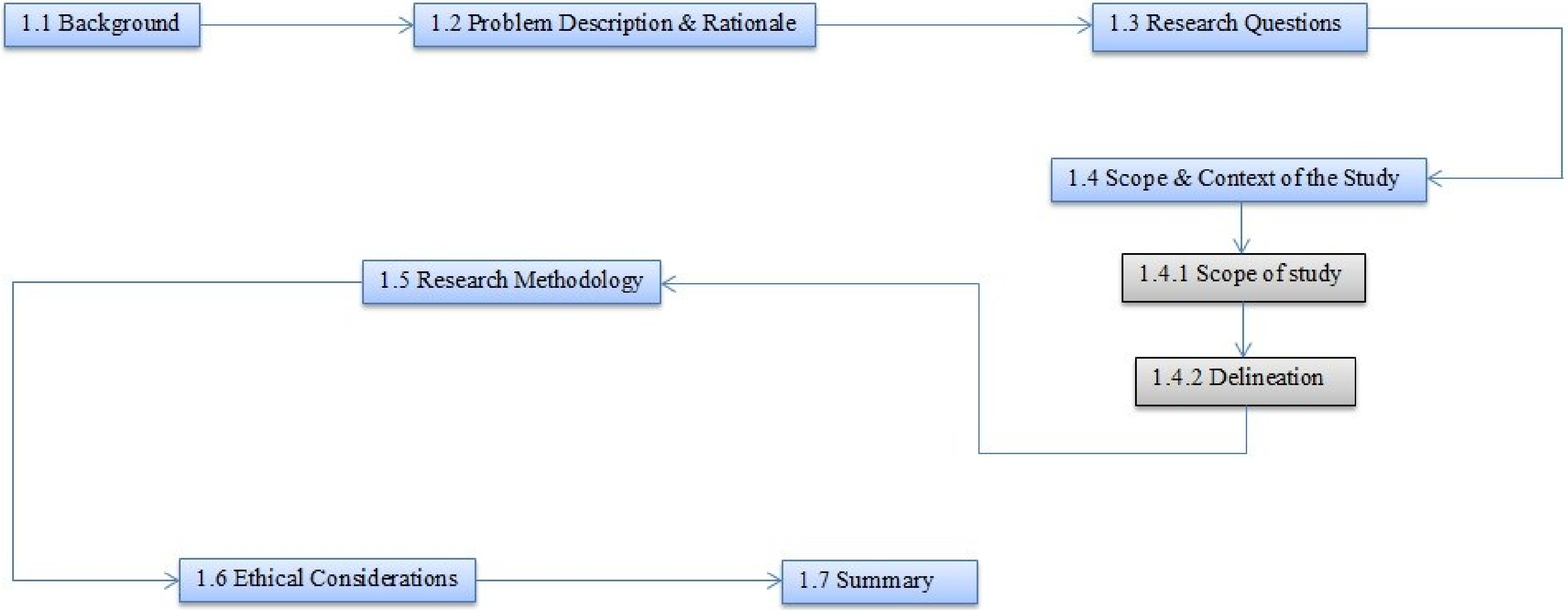
The following publications stemmed from work in the authors Masters Degree, which helped him build and expand his knowledge in the field of Human-computer interaction:

1. Van Greunen, D & Yeratziotis, A. (2009). e-Government: Putting service at your fingertips, IST-Africa 2009, Kampala, Uganda.
2. Yeratziotis, A. & van Greunen, D. (2008). e-Government: Living up to the challenge of culture context, SAICSIT 2008 conference, 6–8 October 2008, Wilderness.
3. Yeratziotis, A. & van Greunen, D. (2008). e-Government: The challenge of delivering best value to the people, 10th ZA-WWW conference, 2–5 September 2008, Cape Town.

NOTE:

- All papers were peer reviewed and are included in the Appendices CD-ROM.

LAYOUT OF CHAPTER 1



CHAPTER 1: INTRODUCTION

1.1 BACKGROUND

Over recent years, the growth of the Internet has accelerated. It is estimated that there are currently over two billion users that have access to the Internet (Internet World Stats, 2011). This growth has been driven by developments in technology and people's appetite for absorbing and sharing information and entertainment.

Social networks have recently been identified as one of the most popular form of communication online (Gartner, 2008; Madden & Zickuhr, 2011). Today, social networking is as routine as sending an e-mail at home or work. Research is being undertaken across a set of academic disciplines to examine the nature and implications of this popular medium. The importance of the network structure, as well as the behaviours and motivations of member individuals and organisations, are gradually becoming better understood. However, there is relatively little work that links the behaviours of individuals with specific features in social networks, particularly given the complexity of the multiple devices and contexts of use.

Web 2.0 social networking sites are broadly defined as those websites that rely primarily on their users for content and allow users to make visible connections to each other. There are a few common features shared by these sites. Users are often encouraged to create a profile listing their interests and other personal information. Users are also usually permitted to upload content, such as photos and videos, to the site. Most importantly, these sites encourage interaction by users, including commenting on each other's postings and uploading content (Frost & Massagli, 2008).

Online social networks are characterised by rich content and collaboration between users. A large amount of the content on these sites, ranging from personal data to multimedia files, is contributed by arbitrary Web users. As part of the collaborative aspects of these sites, users are encouraged to post comments on other users' profiles and pages. However, social networking is a disruptive technology that has changed the way people communicate. Employees exchange updates on Facebook and Twitter, log opinions on blogs, and upload snapshots to photo-sharing sites. Beyond Facebook and Twitter, social networking comprises a wide range of Web 2.0 tools. In addition, public social networking media include blogs, wikis, map-based mashups, and social news sites (Boulos & Wheelert, 2007). Anyone can access these networks from work, home, or on the road and users can disseminate any type of information, be it public or private, fact or fiction.

Social networking can bring competitive advantages to a business, for example, including real-time sharing of information and analysis, better collaboration, and an enriched relationship with customers (Gartner, 2008; Madden & Zickuhr, 2011). Consumers now broadcast their thoughts and actions to an ever-widening audience of friends, family, and followers. As the user base of social networks increases – Facebook alone has more than 800 million members – the scope of the networks is also expanding (Facebook, 2011).

Consumers use social networking to make purchasing decisions, corporations promote new products and services with tweets, and customer service takes on a life of its own. Social networking can also make employees feel valued, connected and an important part of the community. Social networking is also being used to provide public related services, such as for health. All of these interactions occur beyond traditional company walls and firewalls, extending the secure perimeter of the corporate network into remote locations and into employees' and consumers' homes (National Cyber Security Alliance, 2011a). Yet there are high-risk hazards associated with social networking. Network attacks, data leakage and theft, reputational damage, and compliance issues are hazards that must be addressed. Due to these risks, users cannot afford to disregard issues of security and privacy in social networking environments (Palo Alto Networks, 2010; National Cyber Security Alliance, 2011b).

The provision of effective security for social networking requires experience in user behavioural change and knowledge of data classification, Web applications, and enterprise security, as users may easily leak critical (and regulated) information via social media. Moreover, ambitious cybercriminals can gain access to sensitive data by infecting networks with malicious code that connects to Web 2.0 platforms, such as Facebook and Twitter. These threats are abetted by the very nature of social media, which is built on flexible Web architecture that enables exploitation and compromise.

Cybercriminals have acknowledged that Web 2.0 platforms are becoming increasingly powerful and open, and enable more sharing of rich data. Such an extraordinarily dangerous combination leaves the enterprise vulnerable to hacking, viruses and malware (Palo Alto Networks, 2010; National Cyber Security Alliance, 2011b). It has become alarmingly commonplace for hackers to unleash malicious code on social media sites to attack networks with viruses, spam, phishing expeditions and Trojan horses.

A study by the Verizon RISK Team (Baker, Goudie & Hylender, 2010), reports that 28% of security breaches in 2010 employed social tactics. This represented a dramatic increase of 16% since 2008. Numerous paths can be used to employ social tactics, with the most common path being email, while the path of social networking websites was employed in 5% of the cases. Owing to the ever-increasing growth of social networking websites, their more established use as corporate assets and the nature of trusting friends, it is expected that criminals will be employing this path for data breaches over the next few years (Baker et al., 2010).

1.2 PROBLEM DESCRIPTION AND RATIONALE

People have always had the need to protect themselves and their assets, as their physical safety and possessions may be at risk of an attack or damage. The use of information technology is no different. There are many types of threat from which users' physical and data assets must be protected. To assist in this protection, industry has developed a range of security mechanisms which make an attack more difficult and will also limit its consequences should one occur. These mechanisms are effective; but users need to understand how to use them correctly.

The human element is critical in the course of an interaction, but it is also a vulnerable one. Attackers have acknowledged this and have paid more attention to it than designers. They have exploited this element and used it to their advantage, making their attacks easier and more fruitful (Sasse & Flechais, 2005). Users find security and privacy difficult to understand and they are, typically, a secondary goal that prevents them from focusing on their main tasks (Whitten & Tygar, 2005). Yet, it is essential to attend to these issues, if they are to protect their information successfully. Owing to the complexity of such measures, users avoid interacting with the available security and privacy features on websites and applications; consequently providing attackers with an even greater advantage.

It is important that users understand the need to adopt more secure online behaviours. Yet, it is unreasonable to expect them to have the knowledge and skills to protect themselves from all threats. Accordingly, the developers and research community have an obligation towards users and should assist them in protecting themselves, as they require guidance and education. Understanding humans and their abilities and considering user-centred design approaches in development can make effective security and privacy mechanisms more usable as well. This will increase their effectiveness because users will have the tools to protect themselves, they will become easier to utilise and people will understand how to use them correctly. This will yield mechanisms that are workable in practice, also preventing users from being the “weakest link” in the security chain (Sasse & Flechais, 2005).

Knowing the threats and low-cost tips for online-secure behaviours is helpful but it is not sufficient, as these are only the initial steps; moreover some of the tips require further exploration. One has to ask whether it is adequate for a business owner to be aware of threats and to educate employees about security alone, or whether it is logical for a home user to have several difficult passwords for several different accounts, and to write them down and store them somewhere. This is not usable nor is it secure. Moreover, is it actually less secure to have automatic software and security updates? Or, if it is usable from the users' perspective, whether a business should configure the strictest security settings on Internet browsers?

The reality is that current security and privacy features make unreasonable demands on users, system administrators and developers alike (Sasse & Flechais, 2005). Accordingly, keeping a system's or users' personal information secure involves an increasing amount of complexity. Developers struggle because they are not aware of the security implications of their design decisions; yet, they are the ones left with the responsibility for making security decisions and designs for new applications and websites.

Security and privacy features that have a usable design will improve users' security behaviours. Users have the ability to learn and use an application or website quickly, if they like it and if it is usable. Facebook has over 800 million active users (Facebook, 2011). Of those, very few were actually trained to become expect users. In using websites like Facebook, users firstly need to understand the importance of security and privacy, which is challenging. Once they have done so and decided to take the measures needed to secure their profile or information, the security and privacy features must be usable. Otherwise, users will not secure themselves effectively. When this occurs, developers and researchers are accountable because they have failed the users. The developers who create great applications and websites that many users interact with daily, have the ability to develop usable security, if provided with the appropriate assistance. Collaboration is therefore required between industry and research to provide developers with tools for developing usable security. Developers can then design effective security measures and deploy them in their applications and websites for the users.

Online social networking environments are a prime example of spaces where there is a critical need for usable security. The potential contributions of usable security to the private and public sectors provide optimistic prospects; however, the security and privacy of information (personal and organisational) remains a legitimate concern. This is even more the case in networked environments that are based on open dissemination of information.

The need for a privacy framework in social networking environments has been emphasised, as it is seen as a possible solution to conflicting privacy issues (Boyd & Ellison, 2007; Preibusch, Hoser, Gurses & Berendt, 2007; Hodge, 2006). Taking this into account, the purpose of the study is to develop a framework for evaluating usable security to address the usability and user experience issues that users face with regard to the security and privacy features available to them in these environments.

Theories and evaluation tools for usable security, including guidelines and principles, are limited and those that exist are at an elementary and progressive stage. As a result, developers struggle to design security and privacy that is usable. Moreover, usable security is a relatively immature field that needs further development. Hence, the topic lends itself to qualitative research (Johnston, 2004). Research in this field is critical, considering the fact that security and privacy tools are regarded as too complex for users to understand and apply. Usable security is discussed in chapter 3.

To evaluate designs for their usability and user experience, usability inspection methods have been implemented in the field of human-computer interaction. Since usability and user experience are crucial to usable security, usability inspection methods provide a platform for developing an evaluation tool that is specific for usable security. The usability inspection method that is considered for the development of a usable security evaluation tool is a heuristic evaluation and human-computer interaction and usability inspection methods will be discussed in chapter 2.

It is well-known that heuristic evaluations are too limited in scope to specifically address the domain of usable security. Consequently, in order to achieve more accurate results in evaluations, heuristics must be developed that can address the requirements of a specific application domain. Therefore, a new heuristic evaluation should be developed that is specific to usable security.

In addition, there is limited literature and no specific approach describing how new heuristic sets should be developed, although new ones have previously been developed for specific application domains by making use of various methods. Therefore, it is necessary to construct a process in which a heuristic evaluation to investigate usable security can be developed. The process must demonstrate the validity and applicability of the heuristic evaluation, as this was a concern of those that were formerly developed. Owing to the nature of this research, the process will centre on a qualitative approach.

From the above discussion, the following issues can be extracted, which substantiate the problem description and rationale for this study:

- There is a need to understand the security and privacy requirements for online social networking environments from a user perspective.
- There is a lack of evaluation tools that can assist developers in designing usable security on websites and applications.
- To our knowledge, there is no qualitative process that clearly demonstrates how to design heuristics for a specific application domain.
- There is no framework that evaluates usable security in online social networking environments. Hence, there is a need to understand the rationale for an effective usable security framework, as well as what must be incorporated in it.

The primary objective of this study is to consider these issues and develop a framework for evaluating usable security. This will ensure that security and privacy features on websites and applications address user requirements from a usability and user experience perspective.

As highlighted, there is currently a paucity of knowledge and research in the literature pertaining to usable security. Hence, the focus of this study is to address this gap. This study will investigate the fields of human-computer interaction, information security and usable security to determine the requirements and components that are needed to develop a conceptual framework for evaluating usable security. This framework will benefit users and developers alike and is anticipated that it will prove to be a theoretical guide for developers by providing them with the ability to enhance their designs for the intended users. This will be achieved by ensuring that security and usability form a unified process that is considered in user interface design. As a result, user competencies and preferences will be acknowledged, leading to higher levels of usable security. This should, in turn, assist users in protecting their information more effectively and provide a more positive user experience. Accordingly, this substantiates the purpose of the framework.

1.3 RESEARCH QUESTIONS

The primary research question of the study was the following:

What are the components of a framework to qualitatively evaluate usable security?

The primary research question is supported by four research sub-questions:

1. *Which usability inspection method can be adapted to evaluate usable security?*
2. *Which approach can be followed to develop the method?*
3. *How can the validity and applicability of the method and approach be tested?*
4. *How can the method and approach be constituted into a framework?*

1.4 THE SCOPE AND CONTEXT OF THE STUDY

There is a need to restrict the scope of the study. The following two sections focus on the matters of limiting scope and delineation of the study.

1.4.1 Scope of the Study

The framework for evaluating usable security was derived on the basis of a qualitative study. This research includes a case study that was conducted on two online social networks in the health context. Within the design of the system, these websites are embedded with social networking tools and capabilities. Accordingly, their purpose is to promote collaboration and free sharing of information between patients and health care providers (Purdy, 2008). Nevertheless, users are concerned about the security of their information and this therefore remains a key priority in, and may be a contributing factor to, the adoption of these websites. It is essential that users are provided with security and privacy features that are as easy to use as they are effective. An extensive discussion on online health social networks will be presented in chapter 6.

The focus of the case study was on the security and privacy features that are available on the websites. Further research is needed to generalise these results because the level of usable security will differ among online health social networks. Nevertheless, it is the usable security heuristic evaluation that assists in determining the usability of security and privacy features. By evaluating more online health social networks with the usable security heuristic evaluation, it will be possible to determine a minimum acceptable level of usable security. This can provide the essential usable security requirements when designing or improving security and privacy features in the context of online health social networks.

Subsequently, a validation tool was developed and used by experts to assess the usable security heuristic evaluation. The order, analysis and triangulation of the data are based on a new approach to develop heuristic sets for specific application domains.

1.4.2 Delineation

A formative usability evaluation was conducted as part of the case study. Online health social networks were selected because they attract a wide range of users who possess different characteristics, desires, cultural backgrounds, preferences and expectations. The benefits of online social networks in health are well emphasised (Purdy, 2008). However, attention has been focused on readiness to address the related cultural, legal, managerial and technical implications. From a legal perspective, there is uncertainty surrounding the security and privacy of users' personal health information (Purdy, 2008).

The current approach to usability and user experience when performing security-related tasks in the context of online health social networks must be evaluated. Accordingly, what is required is an understanding of the security and privacy considerations involved from the perspective of usability and of designing a positive user experience. Moreover, these must be considered in parallel with the actual security concerns surrounding the context.

The research was conducted in South Africa, with the formative usability evaluation being conducted in Port Elizabeth with postgraduate students from the School of ICT at the Nelson Mandela Metropolitan University. The formative usability evaluation and the related results are discussed in chapter 6. The findings obtained from the validation tool are based on the practical experiences and theoretical knowledge of experts in the fields of human-computer interaction, information security and usable security. The validation tool and the results thereof are discussed in chapter 7.

1.5 RESEARCH METHODOLOGY

The research study follows an interpretivist research philosophy and is supported by an inductive reasoning research approach. In addition, a case study was used as research strategy to complement the research approach. Hofstee (2008) and Creswell (2009) support the idea of using a combination of qualitative and quantitative methods in a research study. This study mainly applies qualitative methods, as it originates from the field of human-computer interaction. The weakness with qualitative research is that it can be subjective in that the researcher's opinions can also influence the results. To combat this, several techniques and procedures are used. These include secondary data, questionnaires, heuristic evaluations and a formative usability evaluation. These were conducted with experts and users in order to eliminate bias. Furthermore, using multiple techniques and procedures promotes better data triangulation, which substantiates the validity of the results.

The four research sub-questions are presented in table 1.1. Their objectives and the techniques that will be used to answer them are also provided. The research design and methodology is discussed in detail in chapter 5.

Table 1.1: Overview of research questions with their objectives and techniques

#	Research question	Objective	Technique/Procedure
1	Which usability inspection method can be adapted to evaluate usable security?	Investigate usability inspection methods and determine the method for adaption.	Secondary data
2	Which approach can be followed to develop the method?	Investigate heuristics that were developed for a specific application domain and determine a new process for developing heuristics for specific application domain.	Secondary data
3	How can the validity and applicability of the method and approach be tested?	Develop a validation tool to assess the method and apply the method in the context of online health social networks. Follow the approach to develop the new method and publish a paper on the approach.	Secondary data, heuristic evaluation, formative usability evaluation, questionnaires
4	How can the method and approach be constituted into a framework?	Determine the components for the usable security framework and connect them in a coherent body.	Secondary data, heuristic evaluation, formative usability evaluation, questionnaires, data triangulation

1.6 ETHICAL CONSIDERATIONS

Ethical considerations must be taken into account in the research process. Such considerations focus on what is morally correct or incorrect when conducting research and are affected by the circumstances in which the research is undertaken. This relates to the fact that humans differ in terms of their beliefs and cultures (Babbie & Mouton, 2001). Therefore, what is acceptable in a certain sphere of life may not be in another.

In research, it is the participants' right to be fully informed so that they can make an educated decision about participating or not (Lues & Lategan, 2006). This ensures that they volunteer to participate and are not forced to do so against their will, while being fully aware of any possible consequences. Just as the consequences of the study are communicated, so must the aims. Additionally, participants' must be allowed to withdraw at any time and they must not be subjected to any type of harm or danger, physically or psychologically.

An important ethical consideration is confidentiality. This must be provided where necessary or desired. In this research study, informed consent was required for the formative usability evaluations and this was acquired before the formative usability evaluation was conducted. The aims of the formative usability evaluation and of the research study in general were communicated to the participants, who were also informed that they had the right to withdraw from the formative usability evaluation at any time. All participants agreed and signed informed consent forms. These are confidential and will be kept by the promoter of this research study for a period of two years. Examples of the two consent forms that each participant signed are included in the Appendices CD-ROM. These are presented in *Appendix B.43: Consent Form for MedHelp* and *B.44: Consent Form for Google Health*.

1.7 LAYOUT OF THESIS

The thesis is divided into nine chapters. Chapter 1 is the introduction and provides an overview of the research. Moreover, it outlines the problem, the research questions, the methodology and the scope and limitations of the study. Chapters 2 and 3 are the theoretical chapters and provide the contextualisation and background information, which facilitates the conceptualisation of the research study. In chapter 2, the focus is on human-computer interaction and in chapter 3 a detailed overview is provided for usable security.

Chapter 4 presents the process for developing heuristics for a specific application domain and the usable security heuristics with their checklist items. The research design and methodology follow in chapter 5. This is an extensive chapter that covers research philosophies, approaches, strategies, choices, time horizons and techniques and procedures. Those selected to be applied in this research study are emphasised, explained and supported.

A case study is presented in chapter 6. The case study was conducted on two online health social networks and the results of the case study and the recommendations flowing from it are discussed. Chapter 7 presents the results and analysis of the experts' assessments of the usable security heuristic evaluation. These experts used a validation tool that was developed in this study to conduct their assessments. In chapter 8 the applicability of the framework is described. Consequently, the contribution of the thesis is highlighted in chapter 9, which summarises the findings and identifies possible avenues for future research. The research process is illustrated in figure 1.1, which also presents the layout of the chapters graphically and identifies where the four research sub-questions have been addressed. In the next chapter human-computer interaction is explored.

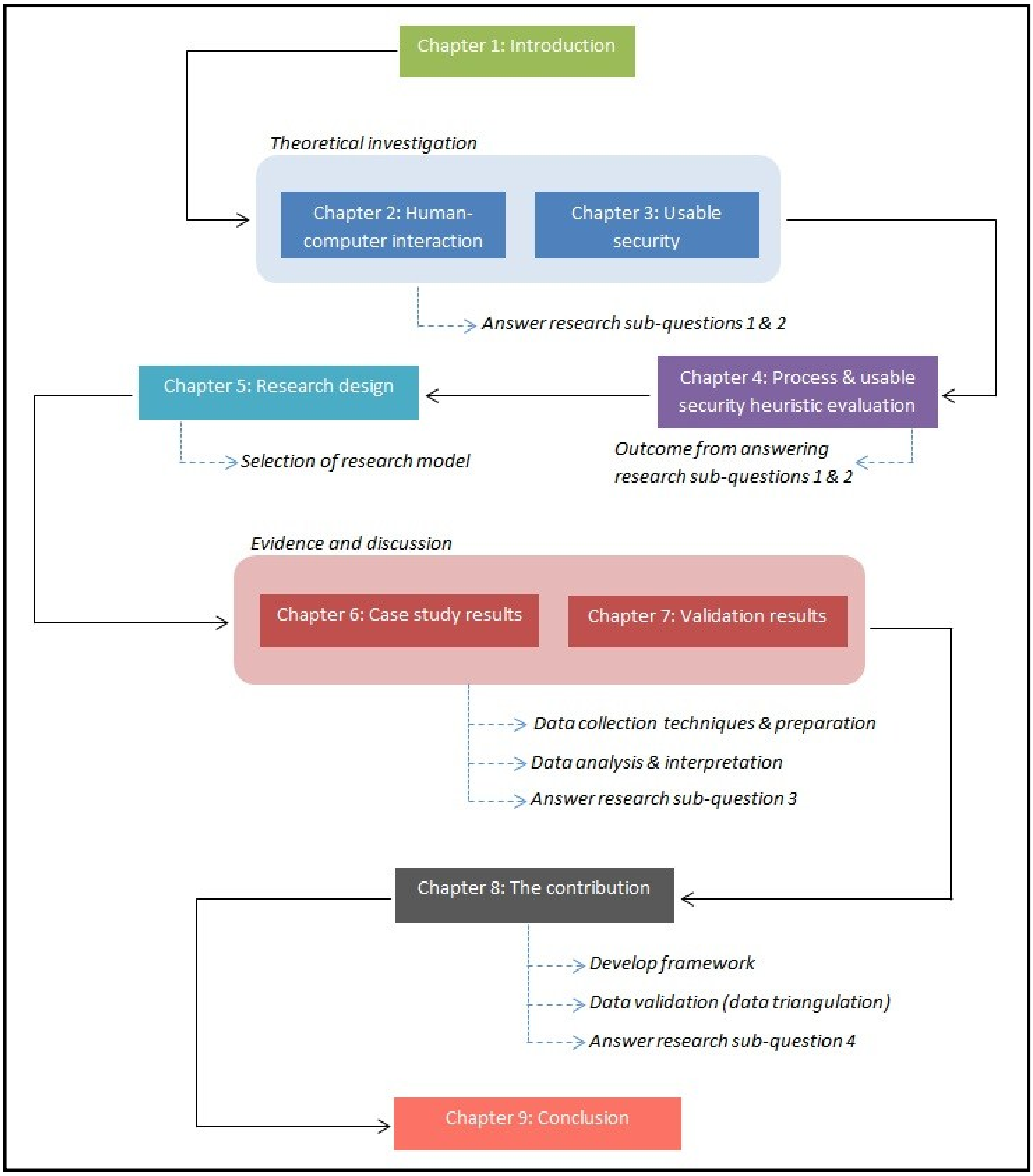
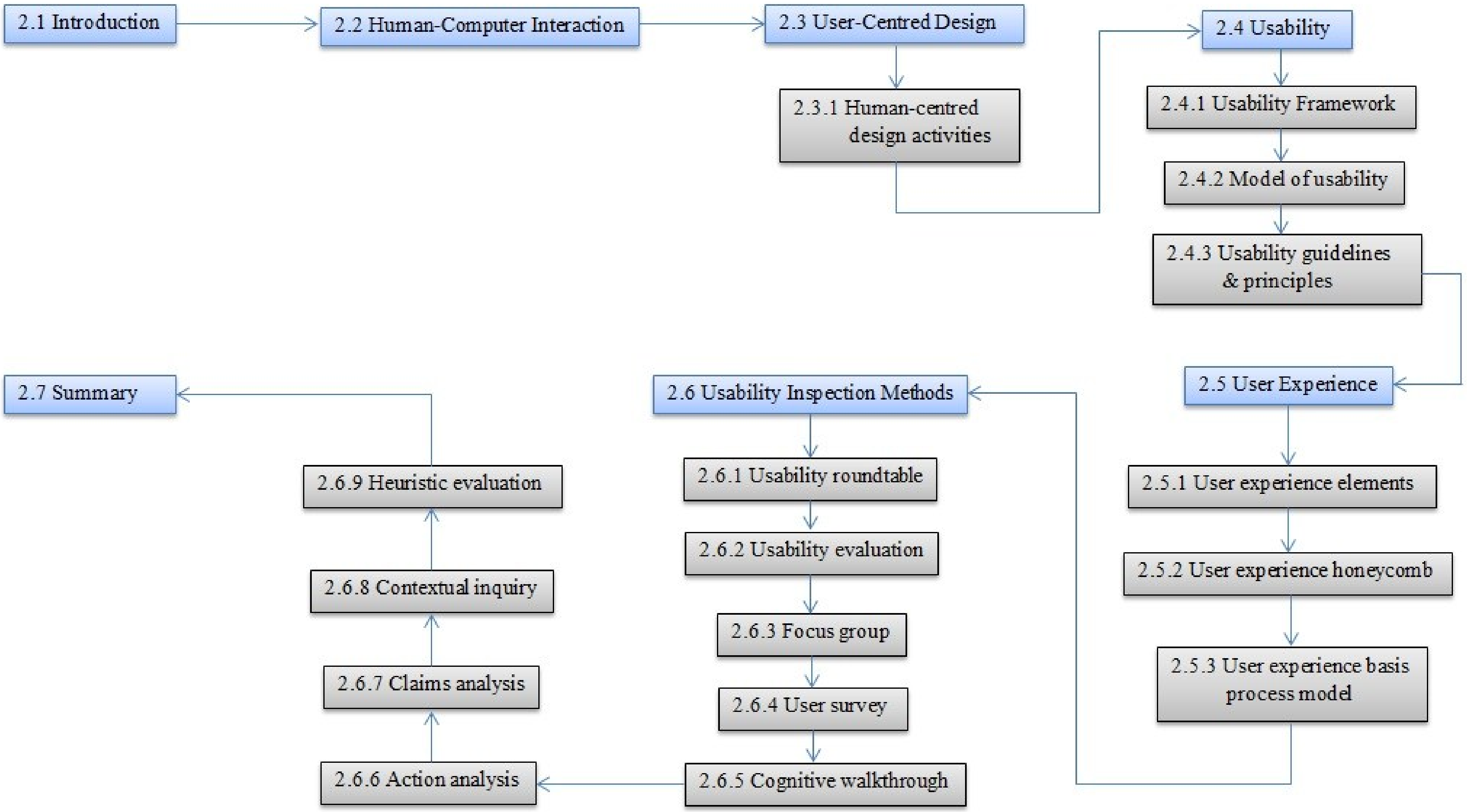

Chapter 1: Introduction
Theoretical investigation
Chapter 2: Human-computer interaction
Chapter 3: Usable security
Answer research sub-questions 1 & 2
Chapter 5: Research design
Chapter 4: Process & usable security heuristic evaluation
Selection of research model
Outcome from answering research sub-questions 1 & 2
Evidence and discussion
Chapter 6: Case study results
Chapter 7: Validation results
Data collection techniques & preparation
Data analysis & interpretation
Answer research sub-question 3
Chapter 8: The contribution
Develop framework
Data validation (data triangulation)
Answer research sub-question 4
Chapter 9: Conclusion

Figure 1.1: Chapter layout of thesis

LAYOUT OF CHAPTER 2


2.1 Introduction
2.2 Human-Computer Interaction
2.3 User-Centred Design
2.3.1 Human-centred design activities
2.4 Usability
2.4.1 Usability Framework
2.4.2 Model of usability
2.4.3 Usability guidelines & principles
2.5 User Experience
2.5.1 User experience elements
2.5.2 User experience honeycomb
2.5.3 User experience basis process model
2.6 Usability Inspection Methods
2.6.1 Usability roundtable
2.6.2 Usability evaluation
2.6.3 Focus group
2.6.4 User survey
2.6.5 Cognitive walkthrough
2.6.6 Action analysis
2.6.7 Claims analysis
2.6.8 Contextual inquiry
2.6.9 Heuristic evaluation
2.7 Summary

CHAPTER 2: HUMAN-COMPUTER INTERACTION

2.1 INTRODUCTION

This chapter will focus on the field of HCI. There are a number of terms and disciplines that are used in this field: of particular interest to this research are the disciplines of human-computer interaction (HCI), user-centred design (UCD), usability and user experience (UX). These disciplines will be considered for the design and development of the Usable Security (USec) heuristic evaluation (HE) and for the process of developing HEs for specific application domains (SADs). The models and frameworks that are presented in each discipline contributed in the development of the framework. There is a broad volume of literature pertaining to these disciplines; however, reference is only made to the literature that had a direct impact on this research study. The disciplines will be introduced in this chapter and a discussion on their relations is also provided.

Section 2.2 will introduce the field of HCI. Subsequently, UCD is discussed in section 2.3. Section 2.4 introduces the discipline of usability and in section 2.5, UX will be discussed. Following this, is a discussion on evaluation methods used in HCI in section 2.6. The summary is presented in section 2.7.

2.2 HUMAN-COMPUTER INTERACTION

Simply stated, HCI is the field concerned with improving the design and development of websites/applications for users. The ACM SIGCHI Curricula for Human-Computer Interaction defines HCI as the following (Hewett, Baecker, Card, Carey, Gasen, Mantei, et al., 1996, p. 5):

> *"HCI is a discipline concerned with the design, evaluation and implementation of interactive computing systems for human use and with the study of major phenomena surrounding them."*

The purpose of HCI is to achieve a certain level of performance in terms of the quality and optimality of a service. In order to realise this, a fit has to be produced between the user, the machine and the actual service. Determining whether an HCI design is good is largely subjective and dependent on the context (Te'eni, 2006). The human, computer, use and context are the main characteristics in the development process. Figure 2.1 gives a representation of the nature of HCI (Hewett et al., 2002).

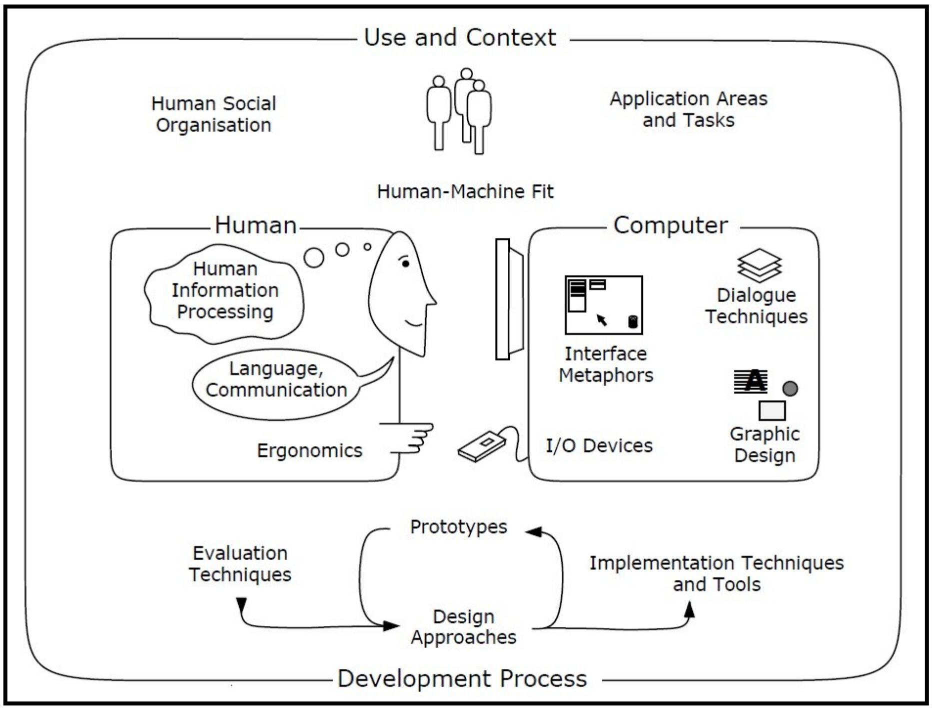


Figure 2.1: The nature of HCI (Hewett et al., 2002, p. 13)

In the process of HCI design, the degree of activity between the human and the computer must be well-thought through. User activity has three different levels: these include physical, affective and cognitive. Accordingly, the physical aspect focuses on the mechanics of interaction between the human and the computer; the cognitive aspect focuses on the ways in which the human can understand the system and interact with it; and the affective aspect focuses on making the interaction a pleasurable experience for the human and ensuring that the human continues using the machine. This aspect depends on emotions and attitudes (Karray, Alemzadeh, Saleh & Arab, 2008).

HCI is an extensive subject area that includes a number of terms and disciplines, as previously mentioned. These are either used interchangeably or applied to complement each another during design. Nonetheless, they all share the common goal of improving the intended users' experience by making them the focal point of the design. Some of the more familiar disciplines are UX, UCD, user interface (UI) design, interaction design (ID), information architecture (IA) and usability. Their objectives can overlap as a result of their interdependencies.

Owing to the terms and disciplines that exist in the area, it is difficult to provide a definite consensus on their relationships. Literature indicates different views with regard to this, yet not necessarily conflicting ones. This has become even more complicated by the surface of

UX. Accordingly, extensive research has been conducted to define UX design and its role with the other disciplines. Therefore, it is appropriate to provide a stance on the perspective that is taken in this research study, as this will enhance the understanding of this chapter in terms of the disciplines discussed.

With regards to HCI, Saffer (2009) states that it has different (non-design) traditions and methodologies in comparison to the other disciplines. This is as a result of its pure research focus. Based on Saffer's (2009) views and because this is a pure research project, this study is positioned within the field of HCI, even though Saffer and the ACM SIGCHI Curricula for Human-Computer Interaction refer to HCI as a discipline as well. Within HCI, this research study will investigate the disciples of UCD, usability and UX. In agreement, Saffer (2009) presents UX design as a discipline that overlaps with all other disciplines and that needs to be considered in each.

2.3 USER-CENTRED DESIGN

The purpose of UCD is to develop products with a high degree of usability. To achieve this, the user becomes the centre of focus in the product development process. Usability is therefore the outcome of correct UCD. Owing to their dependant relationship, it is worth introducing UCD before usability is discussed in section 2.4. UCD is defined as the following (Henry, 2007, p. 29):

> *"UCD is a user interface design process that focuses on usability goals, user characteristics, environment, tasks, and workflow in the design of an interface. UCD follows a series of well-defined methods and techniques for analysis, design, and evaluation of mainstream hardware, software, and Web interfaces. The UCD process is an iterative process, where design and evaluation steps are built in from the first stage of projects, through implementation."*

To better understand the concept on which UCD is founded, it would be beneficial to first compare it to an alternative approach that is used when developing software products, the system-centred design approach (SCD). The design of a new system in SCD is highly focused on the actual characteristics of the system. For example, designing a product that is to run on a particular platform will evidently influence its design process. This is because the new system will need to be designed in such a manner that it optimises and fits into the platform for which it is intended (Leventhal & Barnes, 2007). In UCD, however, the focus of the design is not based solely on the system characteristics, as it is in SCD. Instead, it is based on the fundamental objective to best address the users' needs and tasks. This is the vehicle that drives the design process. The needs and tasks of users must also be in line with what is stated in the requirements documents. It is even possible to sacrifice certain system efficiency in order to address users' needs with regard to their interactions with the interface (Leventhal & Barnes, 2007).

It is evident that UCD depends on the participation of the intended users of a new product throughout the design process. Terms that are used synonymously with UCD are human-centred design (HCD) and user-centred system design (UCSD). ISO 9241-210 (2010), however, states that, in the case of HCD, it also addresses the impact of the stakeholders and not only those of the users, as in UCD. HCD is defined as the following (ISO 9241-210, 2010, p. 2):

> *"HCD is an approach to systems design and development that aims to make interactive systems more usable by focusing on the use of the system and applying human factors/ergonomics and usability knowledge and techniques."*

As with HCD, the definition for UCSD identifies the user as the focal point of the design by stressing the importance of usability throughout the design process. UCSD is defined as the following (Gulliksen, Goransson, Boivie, Blonkvist, Persson & Cajander, 2003, p. 401):

> *"UCSD is a process focusing on usability throughout the entire development process and further throughout the system life cycle."*

Gathering requirements from users and involving them in the design process is not a simple task. Nevertheless, there are various investigative methods that can help the design team accomplish this effectively (Benyon, Turner & Turner, 2005). The most frequently used methods will be discussed in more detail in section 2.6.

2.3.1 Human-Centred Design Activities

As mentioned previously, the terms UCD and HCD are used interchangeably; therefore, discussing the activities involved in HCD is relevant. There are four main activities that compose the HCD approach. These are displayed in figure 2.2. It is also worth noting that the HCD activities will only initiate once it has been confirmed that there is a need to design a new system, product or service. This is represented in the top circle of figure 2.2, referred to as "Identify need for human-centred design".

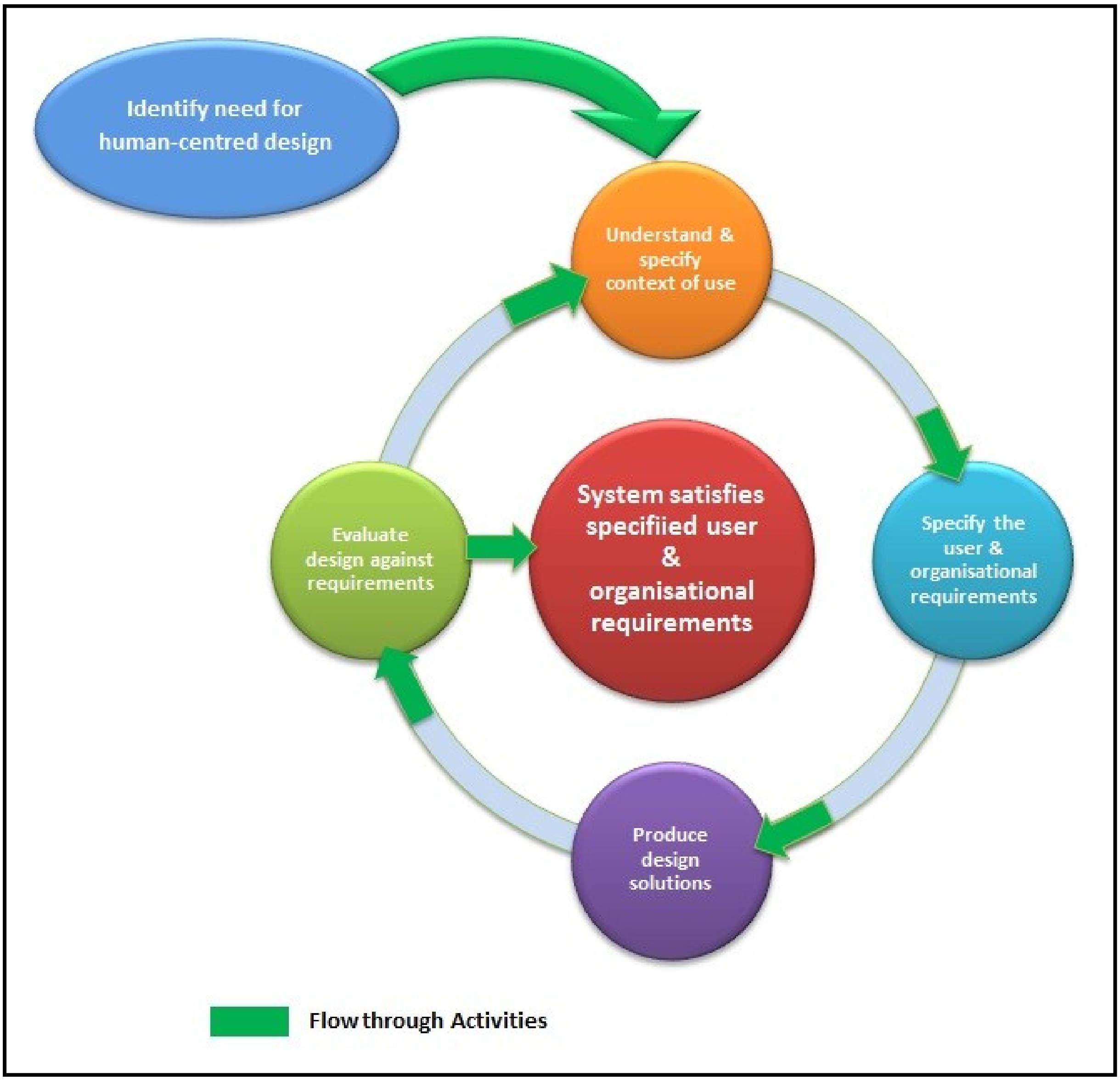

Identify need for human-centred design
Understand & specify context of use
Specify the user & organisational requirements
Produce design solutions
Evaluate design against requirements
System satisfies specifiied user & organisational requirements
🟩 Flow through Activities

Figure 2.2: The interdependence of human-centred design activities (ISO 13407, 1999; ISO 9241-210, 2010)

Once the need for HCD has been established, the next step is to understand the context in which the new system will be implemented. A brief overview of this and the other activities will now be provided. The four activities are the following (ISO 13407, 1999; ISO 9241-210, 2010):

- *Understand and specify the context of use.* Context of use encompasses the characteristics of the intended users, the tasks that the users will need to perform and the environment (organisational, technical and physical) in which the users will be using the system.

- *Specify the user and organisational requirements*. This activity determines and specifies the major requirements of a new system, product or service. It needs to be extended by creating an explicit statement of user requirements. These requirements are dependent on the intended users, context of use and the organisational objectives.
- *Product design solutions*. Potential design solutions are produced as part of this activity. The solutions are based on the description of the context of use, results from any baseline evaluations and the established state of the art in the application domain. Design and usability standards and guidelines, as well as the experience and knowledge of the multidisciplinary design team are all crucial. Iteration is essential at this point and can result in additional user requirements.
- *Evaluate designs against requirements*. User-centred evaluation (from a user perspective) is essential in determining if the human-centred design process is a success. Moreover, new information regarding user requirements may be collected and baselines can be established for comparing alternative designs. User-centred evaluation can provide feedback, which then can also be used to improve a preferred design and assess if user and organisational objectives have been fulfilled. Additionally, it helps monitor the long-term use of the system, product or service.

In chapter 4, the process to develop a HE for a SAD and the USec HE is presented. The HCD activities have been modified in order to provide a platform for developing the process. Additionally, the key characteristics of UCD, which are focused on users, empirical measurements and iteration, are reflected in the process (Gulliksen et al., 2003; Gould & Lewis, 1985; Holtzblatt & Beyer, 1993).

2.4 USABILITY

The relationship between usability and UCD was mentioned in section 2.3. A term that can be used to express this relationship is *usability engineering*. The usability engineering procedure is concerned with two perspectives; the product and the process of the product's development, both of which are equally important. The product focuses on elements such as the content of the user interface, human factor issues, design guidelines and interaction styles. The process, on the other hand, relates to the strategy that was followed to develop the product. This involves methods, techniques and tools for development and assessment (Leventhal & Barnes, 2007).

As with UCD, correct usability engineering is difficult to achieve, as it requires the usability engineer to identify the target users and have a detailed understanding of the tasks they will need to perform. This is a time-consuming process, which is often based on deadlines, and resource and budget constraints. These properties will be adjusted accordingly, depending on the project. Furthermore, the tasks that will need to be designed can be complex. This may even result in conflicting requirements from the user and the organisational perspectives. Another requirement for correct usability engineering is for the usability engineer to constantly make reference to industry standards and documents throughout the usability engineering process (Leventhal & Barnes, 2007).

The usability of products is determined by evaluating whether or not certain usability objectives have been realised in the design of the product. From the website/application perspective, usability objectives include the following (Nielsen, 1993; Rubin & Chisnell, 2008):

- *Learnability (memorability)* – First-time users should have the ability to accomplish basic tasks and infrequent users should be able to relearn the system effortlessly.
- *Efficiency* – Users must be able to perform tasks fast, once they have learnt to use the system.
- *Usefulness* – The product must address the users' needs by enabling them to achieve their goals and perform the tasks that it was designed for.
- *Effectiveness (ease of use)* – Users' speed of performance and error rates are quantitatively measured in accordance with the percentage of users.
- *Errors* – The product should consider and eliminate any errors that the users could be prone to. If any severe errors do occur, the users should be able to recover from them easily.
- *Satisfaction (attitude or likeability)* – Relates to the users' perceptions and feelings on the design and product.

Definitions on usability emphasise the objectives of effectiveness, efficiency and satisfaction as being paramount to the design of the product. Usability is defined as the following (ISO 9241-210, 2010, p. 3):

> *"Usability is the extent to which a system, product or service can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use."*

2.4.1 Usability Framework

Usability is based on specifications and measurements. ISO 9241-11 (1998) states that in order to measure usability it is first necessary to decompose its core characteristics; effectiveness, efficiency, satisfaction and the components of the context of use. These need to be decomposed into sub-components, which will then determine measurable and verifiable attributes. A usability framework distinguishes these components and also illustrates their relationships. Figure 2.3 displays a usability framework.

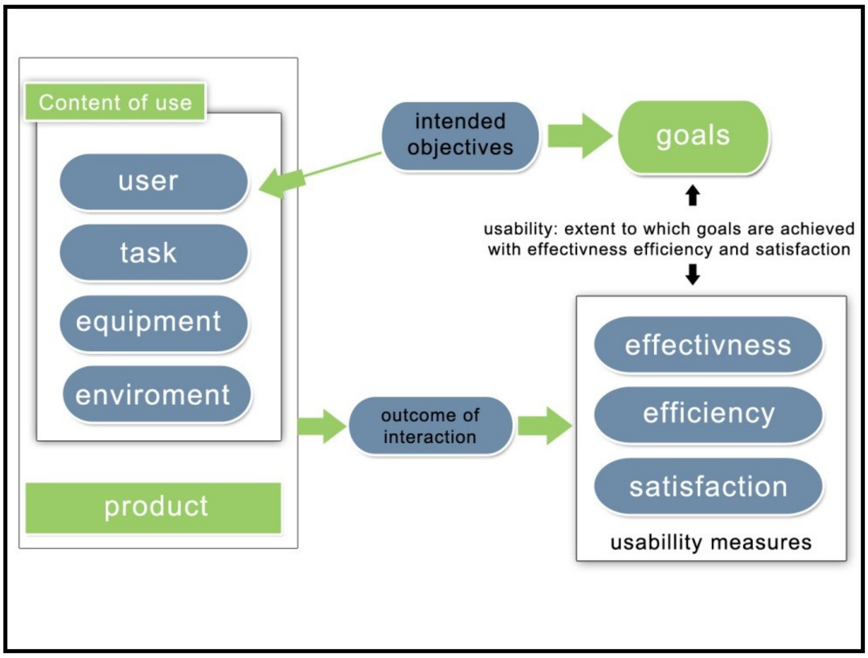


Figure 2.3: Usability framework (ISO 9241-11, 1998, p. 10)

2.4.2 Model of Usability

Models of usability have been introduced by many researchers in the field. They determine the characteristics of usability, how the characteristics interconnect and how the characteristics contribute to the overall usability of a product or service. In addition, they provide a means for measuring usability (as in the usability framework). Common characteristics can be identified within most usability models. The model of usability presented by Leventhal and Barnes (2007) integrates the most important characteristics and variables of several usability models and then combines them into a single model. The model itself is the outcome of an analysis of three other usability models: Shackel's operational model of usability, Nielsen's model of the attributes of system acceptability of which usability is an attribute and Eason's framework for usability.

Consequently, following the structure of these usability models, Leventhal and Barnes (2007) created their own model. In their model, they identify a set of situational and a set of user interface variables. When the two sets are considered collectively they can influence usability. It is worth noting that the model recognises two key aspects within the situational variables – task and user. Variables relating to the task include frequency, rigidness, and situational constraints, while variables relating to the user include expertise and motivation. With regards to the user interface, the variables include ease of learning/use/relearning, flexibility, satisfaction and task match.

The model of usability identifies the type of user interface variables and situational variables that must be considered from both a user and a task perspective. All variables contribute towards usability, an important component for USec, and were therefore considered.

2.4.3 Usability Guidelines and Principles

A number of guidelines and principles exist that can guide and help developers design more usable websites/applications. These make a significant contribution to the design by promoting consistency and good practice throughout. However, applying them alone will have a lower degree of impact without having a good design process in place (e.g. UCD).

An important aspect of the use of guidelines and principles is that they need to be interpreted within a context. Therefore, if a guideline does not apply to a particular website then it should not be implemented. Typically, developers will work through a list of guidelines and mark which do and do not conform to the website/application under development. Hence, guidelines relate to different aspects of the design; home page, task orientation, navigation, information architecture, trust, search, page layout, visual design, help, feedback, errors, and so forth. Some of the most noteworthy resources for usability guidelines include the following:

- Nielsen's ten usability heuristics (http://www.useit.com/)
- ISO 9241 usability heuristics (ISO 9241-11, 1998)
- Usability.gov (http://www.usability.gov/)

- Welie.com (http://www.welie.com/)
- Research-Based Web Design & Usability Guidelines (Leavitt & Shneiderman, 2006).
- Xerox HE checklist (Pierotti, 1995).

2.5 USER EXPERIENCE

Recently, the discipline of UX has been gaining substantial interest within the HCI field. Its contributions stem from the fact that it attempts to consider subjective attributes, such as aesthetics, emotions and social aspects, in the design and development of products. Previously, these attributes were associated with the ease of use of a product. However, nowadays they are being analysed in terms of the users' sensations, behaviours, perceptions and emotions. Researchers have provided various theories and frameworks regarding UX. Consequently, it would seem that the complexity and richness of the UX depends on the diversity of these approaches (Ardito, Costabile, Lanzilotti & Montinaro, 2007).

Ardito et al. (2007) state that although designing for experience includes efficiency, it requires far more. Whereas designing for efficiency would require focusing on attributes such as speed, simplicity, functionality and error-free designs, UX is involved with the users' feelings. Consequently, when using the product the focus is on beauty (harmonious, clear), emotions (affectionate, lovable, erotic), and stimulus (intellectual, motivational). In the design of multimodal interfaces, additional feelings that would need to be considered include touch (smooth, soft) and acoustical (rhythmic, melodious).

In order to understand how interaction impacts and, ultimately, forms experience, Ardito et al. (2007) identify time as having a critical role to play in the users' consciousness. Furthermore, they emphasise the importance of designing actions so that users are not only satisfied with the outcome of their actions, but also with the feelings that ensue from executing them. Hassenzahl and Tractinsky (2006) and Roto (2007) believe that UX is influenced by several factors, including the users' internal state (e.g. expectations, needs, motivation and mood), the characteristics of the designed system (e.g. complexity, usability) and the context surrounding the interaction (e.g. organisational or social setting).

From a commercial perspective, UX design is a specialised discipline that combines product strategy with usability engineering. It is concerned with the interactions between the end-users and a company, its products or services (Nielsen-Norman group, n.d). To achieve this, it is first necessary to meet the precise needs of the consumers. The aim of UX design is to make the product or service useful, elegant and simple to use. The overall experience when interacting with the product or service should be established on the feelings of enjoyment, satisfaction and anticipation (users actions should result in their intended expectations). This will, in turn, drive competitive advantage and profitability. UX is defined as the following (ISO 9241-210, 2010, p. 3):

> *"UX is a person's perceptions and responses resulting from the use and/or anticipated use of a product, system or service."*

2.5.1 User Experience Elements

Garrett (2000) created a conceptual model of considerations for designing successful user experiences for websites. His conceptual model was founded upon his own work and practical experience in the subject area. Within the model he defines elements for UX. In figure 2.4, five layers of elements can be identified.

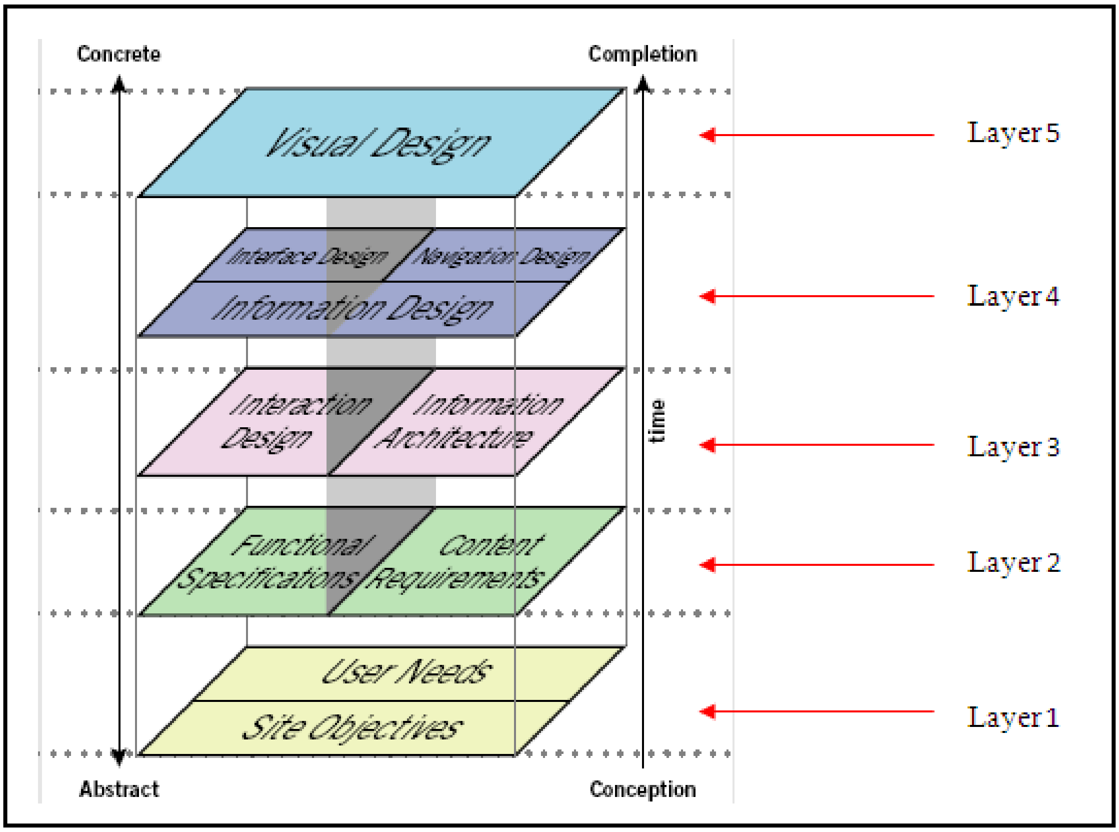


Figure 2.4: The UX elements (Garrett, 2000)

Layers two, three and four are divided vertically. The right-hand side of these divided layers represents the Web as a hypertext system, while the left-hand side represents the Web as a software interface. Of interest in these layers are the left-handed ones because they represent the Web as it is being used today: as sophisticated front- and back-end technologies (Garrett, 2000). When considering these elements in the development of a website/application, they begin at an abstract point. As they move higher up through the levels, concrete artefacts will be built. According to Garrett (2000), the purposes of each layer include the following:

- *Layer 1* – The user needs and the site objectives are identified.
- *Layer 2* – The functional specifications of the site are analysed. This is concerned with describing the functionality of the site in order to meet the user needs that were derived in Layer 1.
- *Layer 3* – This is referred to as interaction design and is interested in how the user interacts with the functionality of the site. Creating the application flows and user tasks are critical for this layer.
- *Layer 4* – This is comprised of two components: the information design element focuses on presenting the information to the users in an understandable format, while the interface design element investigates the design of the interface elements in order to accommodate user-interaction with functionality.
- *Layer 5* – The visual design element is applied. This focuses on the graphic treatment of interface elements and their “look and feel”.

It is apparent from figure 2.4 that there is no element in any of the layers representing usability. This could be explained by defining the element of ID in Layer 3. Hence, interaction design is the process of designing interactive products to support the manner in which people communicate and interact in their everyday and working lives.

Achieving UX is the driving force behind ID. Furthermore, UX is highly dependent on achieving usability goals. Accordingly, these goals need to be considered when designing websites/applications, as they contribute significantly towards the design of a successful product or service. Usability goals are concerned with meeting specific usability criteria such as efficiency, effectiveness, learnability and safety (Rogers, Sharp & Preece, 2008). Based on this, it can be concluded that usability is reflected within the element of ID at Layer 3, as illustrated in figure 2.4.

2.5.2 User Experience Honeycomb

On the basis of an analysis of the UX elements, Morville (2004) then developed the facets of UX, which are referred to as the UX Honeycomb. Currently, there are seven facets and, according to Morville (2004), new facets should be added to the currently existing ones. The seven facets are displayed in figure 2.5 and include the following (Morville, 2004):

1. *Useful* – It is important that the products developed are useful and that innovative solutions are implemented.
2. *Usable* – This relates to the usability of the product or service (e.g. ease of use).
3. *Desirable* – This focuses on the emotional design aspects of a product or service (e.g. images, identity, brand, etc.).
4. *Findable* – This relates to the design of the navigation structure. Users need to find the objects that they require easily.
5. *Accessible* – This highlights the fact that people with disabilities will also need to be considered, as they too can be users of the product or service.
6. *Credible* – This analyses the design elements that will contribute to gaining user trust.
7. *Valuable* – The product or service will need to offer value to both the customers and to the organisation/sponsor.

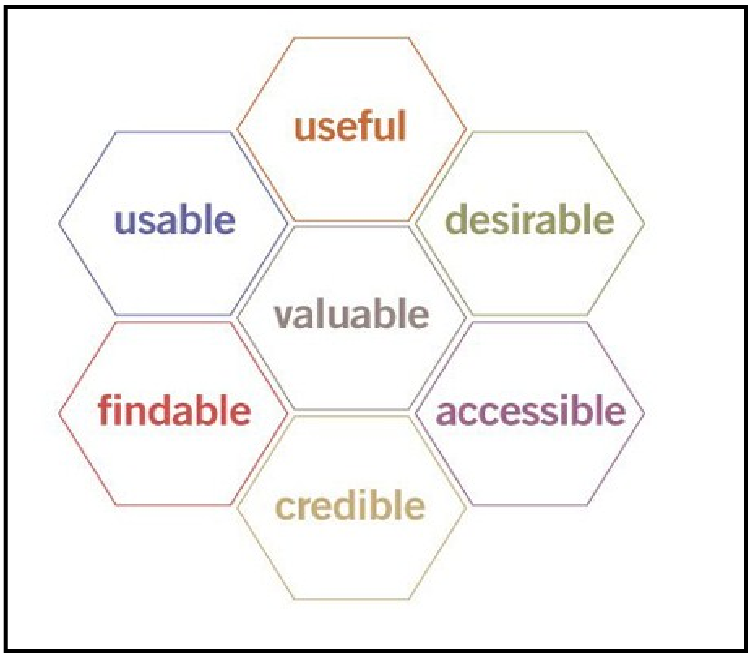


Figure 2.5: The seven facets of the UX Honeycomb (Morville, 2004)

As a result of the development of the USec HE, this research will recommend the addition of a new facet to the UX Honeycomb. The eighth facet being recommended for the UX

Honeycomb is Secure. This facet should be equally considered in the development of websites/applications and is demonstrated in figure 2.6. It is important to emphasise the difference between the Credible facet that already exists and the Secure facet, which is not yet included in the UX Honeycomb. The Credible facet focuses on aspects of persuasion and is interested in determining whether users believe what they read on a website, how users evaluate whether an online source is credible and what the design factors and elements are that influence their opinions of credibility (Web Credibility Project, 2007).

The Secure facet will be concerned with the users' ability to perform security actions easily and to protect their privacy and data when interacting with a website and other users. This becomes even more crucial in websites that utilise end-users' personal information. The objective is to build security tools on websites/applications that will not only protect users and be effective, but which are also easy to use. The security tools will need to be developed in a manner that end-users will understand, so that they may continue to use them. The developers' responsibility is not only to create security tools that work, but also to ensure that their security tools are usable products that can also be applied by novice users. Being able to use the security tools correctly and easily will provide the users with satisfaction, trust and a sense of security. As subjective attributes are essential for UX, including the eighth facet of Secure to the Honeycomb is a legitimate argument.

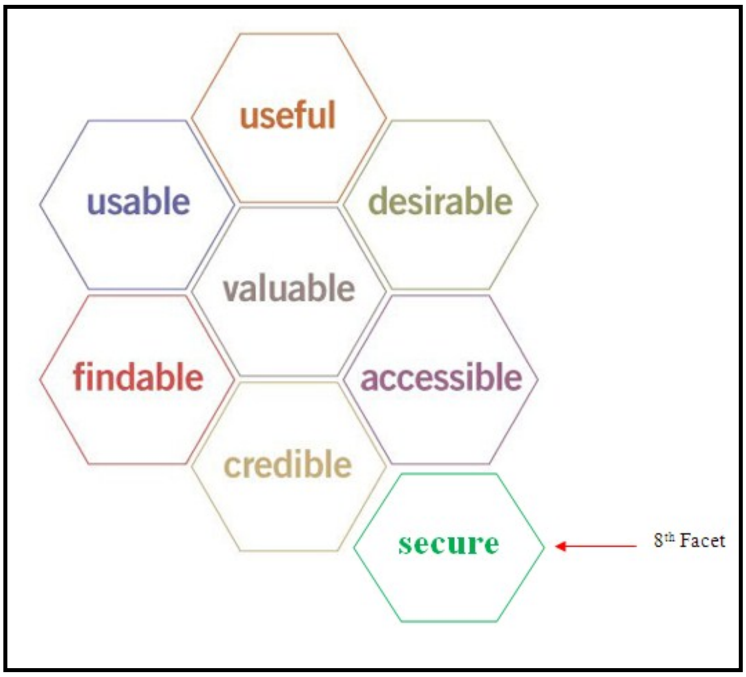


Figure 2.6: The recommended "Secure" facet that will be added to the UX Honeycomb

2.5.3 User Experience Basis Process Model

The UXBasis process model (http://uxbasis.hellogroup.com/) provides an industry perspective for UX design. This process comprises a toolbox that includes 24 different methods that can be used in various situations. The purpose of the toolbox is to promote design with UX at the forefront. It is an adaptive model that is used throughout the development process. The reason for presenting this process model in this research is to understand how UX design can actually be practised in industry and to determine whether there is a correlation with models and processes presented in the literature.

It is evident that the impact of UX is being noted in industry (UXBASIS, n.d.). Hence, companies are trying to design products that provide a positive UX for users. The Hello Group has acknowledged this and has consequently developed the UXBasis process model to assist development teams in their quest for UX design. They state that not all 24 methods are required in a project; only the most relevant that will provide the most effective results for the business need to be utilised. Different methods will be used in different phases of the project, which will undergo constant iterative changes.

The process model is divided into five sections: business intelligence, analysis, structure, interaction and sample and UX is reflected in all these sections. Other HCI disciplines that are continuously reflected in these sections include IA, ID and usability. The methods that can be applied in each section of the UXBasis process model are displayed in table 2.1.

Table 2.1: The 24 methods of the UXBasis process model

Business intelligence	Analysis	Structure	Interaction	Sample
Stakeholder interviews	Task analysis	User journeys	Wireframes	Beta testing
Competitor analysis	Card sorting	Site structure diagram	Page flows	Eye tracking
HE	User interviews	Optimisation	Prototypes	User test labs
Content audit	Ethnography			Think aloud
	Collaborative workshops			
	Web metrics			
	Online surveys			
	Personas			
	User stories			
	Concept model			

The UXBasis process model relates to the respective literature in the research area. The most important characteristics that confirm this is the fact that it is based on an iterative process, it offers a variety of methods that can be used at different phases of a project and it identifies other disciplines within HCI that need to be reflected upon during design.

Several methods have been considered from the UXBasis process model in this research to develop a new process for designing heuristics for SADs and the USec HE. In the business intelligence section, the HE method is considered, while in the analysis section, user stories, online surveys, and task analysis methods are considered and in the sample section, the user test method is considered. Regarding the task analysis method, a modified version is applied. It should be noted that tasks have not been measured against quantitative data; instead, security and privacy tasks have been formulated in combination with user stories to collect qualitative data from the participants. More detail will be provided in chapters 5 and 6 where the research methodology and case study respectively are discussed.

2.6 USABILITY INSPECTION METHODS

> *"Would you fly in an airplane that hasn't been flight tested? Of course not. So you shouldn't be using software that hasn't been usability tested" (Shneiderman, 1995).*

Usability inspection methods (UIMs) are applied to evaluate the usability of applications/websites in the field of HCI. This is achieved by identifying usability problems or violations using an interface. A usability problem is defined as "any aspect of a user interface that is expected (or observed) to cause users problems with respect to some salient usability measure (e.g. learnability, performance, error rate, subjective satisfaction) and that can be attributed to a single design aspect" (Nielsen, 1993). Once usability problems have been identified, they can be prioritised for improvement by management and developers according to their severity. Hence, it is imperative that one can trust the validity of the ratings from the applied UIM. Otherwise, less urgent usability problems may be addressed ahead of the more severe and urgent ones (Law & Hvannberg, 2004).

Other terms used interchangeably with UIMs are *discount methods* (Woolrych & Cockton, 2001), *usability evaluation methods/techniques* (Dix, Finlay, Abowd & Beale, 2004) or *usability evaluation approaches/methods* (Rogers et al., 2008). The term *discount methods* are used because their main goal is to provide the best possible impact on interactive design at the lowest possible cost (Woolrych & Cockton, 2001). According to Dix et al., (2004) *usability evaluation methods/techniques* are either based on expert evaluation or user involvement. Likewise, the three types of *usability evaluation approaches/methods* include usability testing, field studies and analytical evaluation (Rogers et al., 2008). Usability testing measures users' performance and satisfaction when conducting tasks in a laboratory setting on a system in question. Field studies are conducted in natural settings to understand what users do naturally with a system in question, while analytical evaluations are conducted by experts and do not involve users.

From the various terms that can be used to define the methods that evaluate the usability of applications/websites, the term UIM is used in this study. This is supported on the basis that the most important sources referenced in the development of the USec HE refer to them as such. The selection and application of a particular method is mainly founded on determining if it will be conducted with experts or users. Thus, irrelevant of the term used to describe the methods, clarifying if the method is conducted with users or experts is important, and this will be done when discussing various methods in their relevant sections.

Despite the higher-cost involved with using both users and experts in evaluations, it is beneficial. The continuous involvement of users in the design and evaluation phases must reflect the application of usability practices throughout in order to meet their needs (BoK-a, 2005). In addition to user involvement, expert involvement will complement and enhance the design process. Thus, the user requirements will be combined with business requirements in order to achieve effective UX (BoK-b, 2005). UIMs are particularly fundamental for data collection and analysis within the HCI research field.

Development teams can apply UIMs to evaluate different websites/applications. In doing so, they focus on different issues of the design and are conducted throughout the development of a product. A key consideration in this process is for the development team to know beforehand what type of information they are trying to obtain (Benyon et al., 2005). They can then select the most suitable UIM for the specific case.

UIMs can be conducted with users or field experts. When conducting them with users it is recommended to have at least three to five users for a single user group. If there are more user groups identified, the development team will need to ensure that each user group is represented with three to five users. Context is another important consideration with users – it will need to be recreated so that it matches the actual settings in which users are expected to interact with the product (e.g. usability laboratory). When conducting UIMs with experts, results are dependent on their personal experience and practical and theoretical knowledge. These evaluations require a considerable amount of time and close attention to detail in the design. Context is equally important here; however, it is more imperative when conducting evaluations with users. Overall, the best results are obtained by combining UIMs with and without users, as the methods will complement each other. Once the data have been collected, the design team can employ methods and models for the analysis. These are also helpful in communicating the material to the entire design team. Such examples include flow models, sequence models, artefact models, cultural models, physical models, affinity diagrams, storyboards, User Environment Design (UED), paper prototypes, and Graphical Presentation of User Profile (GUP) (Benyon et al., 2005; Kankainen & Parkkinen, 2001).

When conducting UIMs with users, it is critical that the development teams observe, listen and engage with the users effectively. Richer results are obtained when the development team conducts onsite visits to the users' natural environments. However, as previously stated, the context can be recreated in usability laboratories as well (Butow, 2007). Drawbacks can include bias from the development team due to the lack of adequate feedback from the users or a general lack of information from them and misunderstandings. These drawbacks result when there is confusion and when the development team interprets the users' actions incorrectly.

There are two main reasons for conducting UIMs without users. Firstly, the users' time is valuable and the development team should not unnecessarily waste their time. Therefore, when users start evaluating the design, it should be as free as possible from problems and bugs. Secondly, as a result of the experts' practical experience, a good expert evaluation can determine problems in the design that an evaluation with a few users may not expose (Butow, 2007). UIMs without users are categorised into two groups: task-oriented evaluation techniques and task-free evaluation techniques. Task-oriented techniques evaluate an interface as applied to a specific task that the user would conduct with the actual interface. The advantages of task-oriented evaluation techniques are that they focus on interface problems that occur during the work the user does and that they provide an idea of the importance of problems in the context of the job. Their shortcomings are their coverage and their cross-task interactions. Coverage is difficult to achieve because there is never enough time to evaluate every task that the user may perform. Moreover, identifying cross-task interactions is not possible either because tasks are evaluated on their own and not as part of a system of interconnected tasks. On the other hand, task-free evaluation techniques are used to identify problems that task-oriented usability techniques tend to miss (Butow, 2007). Table 2.2 displays popular UIMs that can be conducted with users, experts or both. It also displays those that will be applied in this research.

Table 2.2: Usability inspection methods

#	UIM	Users	Experts	Users & experts	Applied in research
1	Usability roundtable	√			
2	Usability evaluation	√			√
3	Focus group			√	
4	User survey	√			√
5	Cognitive walkthrough		√		
6	Action analysis		√		
7	Claims analysis		√		
8	Contextual inquiry	√			
9	HE			√	√

The UIMs from table 2.2 will be briefly presented and discussed. Detailed discussions will be provided for the usability evaluation and the HE UIM. This is because they will be applied in this research and will contribute significantly in the development of the new process and the USec heuristics. They are also regarded as the most frequently used UIM.

2.6.1 Usability Roundtable

In usability roundtables, customers (or users) visit the evaluators' site and bring with them some of their work artefacts, which help create to a context for evaluating the products usability (Butow, 2007). This is an effective usability evaluation technique for discovering information about the users' work, although it differs from other techniques in that a portion of the users' work environment is recreated at the design team's premises. As mentioned, users are required to bring their own work samples (e.g. data files, applications samples, hard copy printouts). They then sit around a conference table with the design team and explain their work on the basis of their work samples (Butler, 1996).

The fact that the users are describing their work by means of their work samples provides the design team with a thorough introduction into the users' world. It helps identify the type of issues they are currently facing in their jobs and also provides initial indications as to how technology can improve their work. This ensures that the designs will suit their needs (Butler, 1996). A usability roundtable generally has a usability person to moderate the session in the form of an informal discussion.

Usability roundtables will need to be combined with other techniques as well. A critical consideration when conducting a usability roundtable is that the appropriate users are selected. The key advantages of this technique are that the sessions are efficient, users are enthusiastic about attending the sessions, design team members are better informed about the users' needs and the user environments can be reconstructed effectively (Butler, 1996).

2.6.2 Usability Evaluation

Usability evaluation, also referred to as usability testing (Rogers et al., 2008), is a more expensive and time-consuming UIM. Yet, it tends to be more reliable in comparison to other UIMs (Cockton & Woolrych, 2001; Molich & Nielsen, 1990). The purpose is to predesign a usability test and then conduct it in a controlled environment (e.g. usability laboratory) (Butow, 2007). Usability evaluation helps to indicate where problems in the design occur or to compare alternative designs. Sometimes there is a need for more precise and statistically validated data based on quantitative and qualitative data gathered from the evaluation project. Quantitative data can reliably confirm, according to metrics, that one design is better than another. They can also show that error rates are at an acceptable and pre-agreed upon rate according to requirements. To achieve such results, controlled usability evaluations are needed, which can be analysed using statistical tests. This requires a basic understanding of probability theory, experimental theory and statistics (Benyon et al., 2005).

A set of users is asked individually to complete tasks using an interface. During the testing, usability specialists observe and monitor the users, noting in particular aspects such as mistakes, frustration and time delays in completing tasks. Usability testing helps prioritise cost-benefit corrections to the system. In addition, the suggested design improvements are the result of the experts' usability experience as well as the users' experience when conducting the test (Straub, 2003; BoK-c, 2005).

To conduct a successful usability evaluation, guidelines should be followed. It is important to consider these as they will contribute to well-designed usability evaluations. In turn, these will provide the results that the development team have set out to achieve initially from the usability evaluation. The steps involved in conducting a usability evaluation include the following (Benyon et al., 2005):

1. Select the techniques for the usability test.
2. Define the tests to determine what information is needed from the users and how this information will be collected.
3. Design an initial test and conduct a pilot study. When satisfied with the pilot study conduct the real test.
4. Analyse the data and prepare reports and presentations for the stakeholders (the presentation of the analysis will depend on the intended audience).

The second step in conducting a usability evaluation is to define the usability test (as mentioned in the steps above). Defining a usability test has its own steps, which will need to be considered. These include the following (Butow, 2007):

1. Define the goals and concerns.
2. Determine who the test participants are.
3. Select, organise and create the test scenarios.
4. Determine how usability will be measured.
5. Prepare the test materials.

2.6.3 Focus Group

Focus groups help obtain attitudes, reactions and opinions about a company's products and ideas. They are also useful for helping a development team to better understand its customer requirements (Butow, 2007). A focus group is an informal technique that assesses user needs and feelings before interface design and after implementation. Nielsen (1997) suggests that it is more effective when the group consists of six to nine users and the session last for about two hours. The session will also need to be administered by a moderator, who maintains the focus of interests. However, there still needs to be a free-flowing and relatively unstructured style to the session.

Focus groups in particular cannot be used as the only evaluation technique and are relatively poor in evaluating interface usability. They can also possibly produce inaccurate data, as users may think that they require one thing when instead they require another. The development team will need to consider a solution for this (e.g. prototypes, workshops and scenarios) (Benyon et al., 2005). Note that the main purpose of focus groups is not to assess the usability of the design but to discover what it is that the users need from the system.

2.6.4 User Survey

Development teams make use of user surveys (e.g. interviews, questionnaires) to determine what the users would like to see in the product. These are valuable for clarifying user reactions and perceptions. Information collected from the user surveys can also be applied to future versions of a product (Butow, 2007). Essentially, the design team will select a sample group of participants and administer a standardised survey to each of them (Babbie, 2005). A detailed discussion on surveys will be presented in chapter 5.

2.6.5 Cognitive Walkthrough

Cognitive walkthroughs are a task-oriented evaluation technique and therefore fit well with task-centred design. Although this technique tends to be conducted mostly without users, it is said to be more successful when the designers have worked closely with the users. This is because the designers can then build a mental picture of the intended users in their actual environments (Lewis & Rieman, 1994). The main disadvantages of this method are that it is time consuming if applied exhaustively to substantial systems. In addition, there can be difficulties in producing realistic scenarios and action sequences for novel products and there are limitations considering novice users. This is because assumptions are based on theoretical models of human action and goal-directed planning.

Cognitive walkthroughs are a tool for developing the interface and not for validating it. Designers should expect to find aspects of the design that can be improved. This relates to the fact that often users are not thinking what the designers expect them to be thinking when interacting with the design. Therefore, it is a formalised method for imaging the users' thoughts and actions when they use the interface for the first time. These walkthoughs are basically conducted with the assumption that the users are using the system for the first time and that they have no training on the system.

2.6.6 Action Analysis

Action analysis is a task-oriented evaluation technique and requires a detailed investigation of the sequence of actions a user will need to conduct in order to complete a task with an interface. Action analysis is based on two phases. This first phase focuses on the physical and mental steps that a user will perform to complete one or more tasks with the interface. The second phase is to analyse the steps from the first phase and look for any problems (Lewis & Rieman, 1994). There are two methods for conducting action analysis: formal action analysis and back-of-the-envelope action analysis.

Formal action analysis is also referred to as "keystroke-level analysis". This method is characterised by extreme detail in the evaluation and is not easy to conduct. It allows the designer to predict time scales for expert users to perform tasks and forces the designer to take a detailed look at the interface (Lewis & Rieman, 1994). This analysis is conducted in the following manner: A basic task is divided into a number of subtasks; each of these subtasks is then divided into even smaller subtasks. This process continues until the description reaches the level of fraction-of-a-second operations. The end result is a hierarchical description of tasks and the action sequences needed to accomplish them. This method is only appropriate for special cases, as it is very complex.

Back-of-the-envelope analysis does not provide the level of detail that formal action analysis does (e.g. predictions of task time and interface learnability). However, it can reveal large-scale problems that may be lost in the details of formal action analysis. Moreover, it does not require much effort because there is no need to spend substantial time developing a detailed hierarchical breakdown and description of the tasks. This method is most useful when deciding on whether or not to add new features to a system or interface.

2.6.7 Claims Analysis

Claims analysis is a well-respected technique that should be initiated in the early stages of design. It is then used throughout the development process. Such analysis helps extend scenarios by documenting them with "claims" about their design features. The claims document the envisaged positive effects of a feature, as well as the potential undesirable consequences of a feature (Benyon et al., 2005).

Claims analysis is therefore used to analyse the relationship between the design features and the usability of the interface. A claim is a statement about a certain aspect of the design (e.g. location of a button, feedback provided in response to a user action) in terms of its psychological implications, which will reflect how capable a user is of using that aspect of the design. The outcome of claims analysis will be a list of all the design features of the interface and will include all positive and negative implications of the design features in this list. This is a useful approach for selecting among a number of alternative designs and will also provide a set of questions that can be analysed at a later stage when conducting usability evaluation techniques with users. These questions will state how the design should work on the basis of a well-defined set of claims.

2.6.8 Contextual Inquiry

Contextual inquiry is a type of semi-structured interview method used to collect information based on the context of use. At first, standard questions will be asked of the users, and then the interviewer will ask questions and observe the users as they work in their environments. Owing to the fact that users are being observed within their work context, the analysis data are more realistic, unlike laboratory data. This method is based on a set of principles and is generally used at the beginning of the design process. It is also useful for extracting a wealth of information regarding work practices, the social, technical and physical environments, and user tools (Gaffney, 2004; Holtzblatt, Wendell & Wood, 2005).

2.6.9 Heuristic Evaluation

A HE is regarded as an analytical evaluation method, which is undertaken by usability experts. The experts apply a specific set of heuristics or principles to evaluate the usability of a product. This provides an immediate analysis of the website/application, which helps to correct confusing elements in the current design and leads to enhanced UX. The method is widely used because it is an excellent method of diagnostic and perspective analysis for identifying individual problems in a short time period. Specifically, its purpose is to identify problems that are associated with the design of user interfaces. The results are dependent on the experts' broader experience with usability (Nielsen, 2005a; Straub, 2003; Bernardo, 2005).

HEs are not well trusted owing to their unreliability at times. Yet, according to surveys, they are the most used method. It is believed that they will remain as the most popular UIM in the foreseeable future as well (Woolrych & Cockton, 2001; Law, 2007; Rosenbaum, Rohn & Humburg, 2000; Vredenburg, Mao, Smith & Carey, 2002; Baker, Greenberg & Gutwin, 2001; Law & Hvannberg, 2004). An objective of the research is to define a process to design HEs for SADs. Therefore, it is required to have a comprehensive understanding of HEs. With regards to this study, the SAD is USec and the context that they address is the Online Health Social Networks (OHSNs).

A HE, also referred to as an expert review or a heuristic analysis technique, is a UIM that is conducted by experts in the field of usability engineering (Molich & Nielsen, 1990). It requires experts to use their practical skills in combination with their theoretical knowledge of guidelines and standards. Such practical skills would enable them to evaluate the conformance of a particular design. Nielsen (2005a) refers to it as one of the most popular UIMs that allows for quick, cheap and easy evaluation of a user interface design. Based on Nielsen's remarks, it is evident why they remain extremely popular.

Several experts working independently are considered adequate and very effective for identifying usability issues. Nielsen (2005b) is of the opinion that between three to five evaluators are sufficient, as they would be able to discover an average of 75% of usability problems on the user interface. The more evaluators that can be used, the better; however, this would have to be considered on the basis of a cost-benefit analysis. Figure 2.7 displays the percentage of usability problems that can be discovered based on the number of evaluators used. In figure 2.8 the ratio between the benefits and costs is described. Likewise, this is also dependent on the number of evaluators that are conducting the evaluation. From figures 2.7 and 2.8 it can be concluded that using more than five evaluators sees a decline in the ratio of benefits to cost. Therefore, the recommended number of evaluators is typically between three and five.

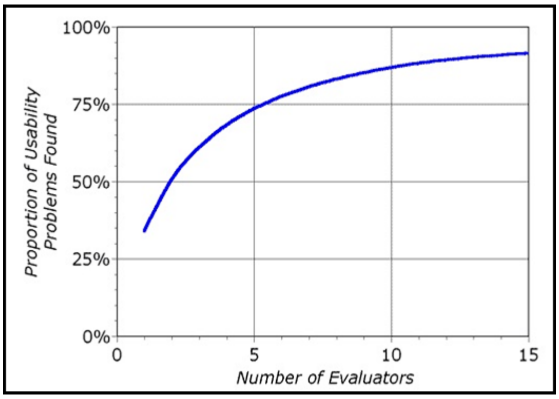


Figure 2.7: Ratio of discovering usability problems on a user interface based the number of evaluators used in a HE (Nielsen, 2005b)

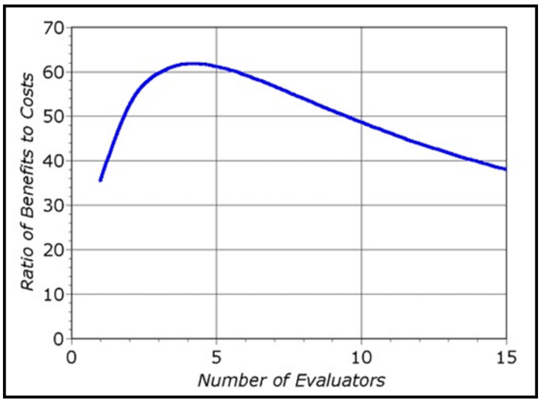


Figure 2.8: Ratio of benefits to costs based on the number of evaluators used in a HE (Nielsen, 2005b)

Experts use a set of heuristics, which are similar to guidelines, to evaluate an interface or prototype. The outcome of their evaluation should be a list of violations and usability issues in accordance with the list of heuristics by which the interface is being moderated (Leventhal

& Barnes, 2007). The identified usability issues can then be addressed as part of an iterative design process. In this regard, severity ratings are used to measure the extent of the usability issues, as they help to determine the most serious problems with the interface and to estimate the need for additional usability efforts. Resources can then be allocated accordingly. Consequently, depending on the ratings, a product may or may not be released. For example, a product that is judged to have usability problems of a cosmetic nature can be released and those problems may then be solved at a later stage. The severity of a usability problem is a combination of three factors: frequency of problem occurrence, impact of problem when it occurs and persistence of the problem (Nielsen, 2005c).

Two popular sets of heuristics that are widely accepted and adopted in an HE are those of Jacob Nielsen and the Xerox Corporation. Accordingly, Nielsen has developed the “ten usability heuristics” (Nielsen, 2006) and Xerox the “HE – system checklist” (Pierotti, 1995). From here on these will be referred to as well-known heuristic sets. Although the two are recognised as separate sets, in essence, the Xerox checklist operationalises Nielsen’s usability heuristics (Ballard, 2010). In many cases, it is possible and sufficient to use one of the well-known heuristic sets and conduct a basic HE on a user-interface. This is very practical, as it is cost-efficient, time-efficient and effective in identifying the major usability issues that do not conform to the well-known heuristic sets of use. This does, however, lead to an argument being raised: that is, whether or not the well-known heuristic sets are considered as a “one-size-fits-all” approach for an HE. Research studies have proven that this is not always the case, as there are cases where heuristics need to be designed for a SAD in order to fit the specific context of use. Currently, there is no literature describing a systematic process that can be followed in an attempt to develop new heuristics, even though HE is an area in the HCI research community that has been well studied. At present, there are two main themes within this space (Sim, Read & Cockton, 2009):

1. Improving the effectiveness of a HE
2. Developing new and novel heuristic sets for specialised domains

This research considers both of these themes. Firstly, it attempts to develop a USec HE that corresponds to the theme of developing new heuristic sets for specialised domains. Secondly, it will provide a new process for creating an HE for a specialised domain. This corresponds with the theme of improving the effectiveness of the HE method. A proficient and systematic process for developing specific heuristic sets will help reveal covert problems with an interface, especially during the initial evaluation phases (Somervell & McCrickard, 2005). This, in turn, will improve the overall effectiveness of this UIM.

There is no consensus about the most effective process for developing heuristics for SADs (Sim, Read & Cockton, 2009). A review of five previous studies that were readily accessible to the researcher points out several methods for doing this:

- The first study suggests two main methods (Paddison & Englefield, 2004). These include examining the literature and analysing data of prior studies.
- The second study suggests three main methods (Ling & Salvendy, 2005). These include examining previous research literature, modifying existing heuristics (referred to as tailored made heuristics) and evaluating the results. The tailored-made method is more common and has been used in the development of heuristic sets for ambient displays and shared workspace groupware applications (Baker et al., 2001). The need to create tailored evaluation tools for other domains is well supported (Somervell & McCrickard, 2005; Hvannberg, Law & Larusdottir, 2007).
- The third study was done by Jacob Nielsen who used two methods to devise his well-known heuristic set (Sim et al., 2009). These methods include factor analysis and an explanatory coverage process. However, his heuristics are regarded as too general in content and limited in scope to address SADs (Law & Hvannberg, 2004). With regard to the design of heuristics, Nielsen states that "it is possible to develop category-specific heuristics that apply to a specific class of products as a supplement to the general heuristics" (Nielsen, 1994). He further recommends that this could also be done by performing competitive analysis and user testing to create abstract categories of specific heuristics. Nonetheless, this remains a complicated process that always raises questions regarding validity.
- The fourth study used a more systematic approach to develop heuristics for SADs (Somervell & McCrickard, 2005; Sim et al., 2009). The approach includes identifying examples in the system class, extracting design knowledge from each representative system, grouping and labelling heuristics and deriving the final heuristics (Somervell & McCrickard, 2005). The work of these researchers is referred to as Study D in table 2.3. Based on this approach, the three key aspects of study are the system class (large-screen information exhibits), the design technique (scenario-based design and usability evaluations) and the knowledge storage approach (claims analysis).

- In common with the previous study, the fifth study used a more systematic approach to develop heuristics. It used an evidence-based or mixed-method approach to create a heuristic set for computer assisted assessment applications (Sim et al., 2009). Accordingly, its design and evaluation process included determining the effectiveness of Nielsen's heuristics within the specialised application domain, building a corpus of usability problems by conducting student surveys, HEs, literature review and synthesising the corpus into a set of SAD heuristics (Sim et al., 2009). The work of these researchers is referred to as Study E in table 2.3.

Studies D and E both used a more systematic approach in developing their heuristics. However, their approach for heuristic development required a significant amount of time. The most time-consuming aspect in Study D was the claims analysis and for Study E was the filtering and merging of the data sets to create the corpus. Both studies support the effectiveness of their heuristics with quantitative data methods. A comparison of these studies with the new process being proposed in this research is presented in table 2.3. The comparison is based on a set of elements, as displayed in table 2.3.

Table 2.3: Comparison of studies D and E with the new process proposed in this research

Element	Study D	Study E	New Process
Time	More time consuming due to the claims analysis technique.	More time consuming due to filtering and merging of data sets into a corpus.	Less time consuming. A validation tool to assess heuristics is provided. However, the experience, knowledge and effectiveness of reviewers and their willingness to contribute make a significant impact.
Approach	Quantitative	Quantitative with some aspect of qualitative techniques	Qualitative
Methods	Mixed method	Mixed method	Mixed method. This allows for data triangulation and differs from the other two studies because it includes the methods from previous researchers and integrates them into the process.
SAD	Large-screen information exhibits (non-controversial)	Computer-assisted assessment applications (non-controversial)	USec (highly-controversial). Therefore a subjective consensus is required.
Evaluations	Usability problems were purposely introduced into the prototypes and	HEs were conducted in the application domain to build the corpus of usability problems.	Users apply the high-level heuristics on the website/application and are also provided with relating tasks to

Element	Study D	Study E	New Process
	systems.		demonstrate the applicability. Experts will use the validation tool to evaluate the high-level heuristics.
Severity ratings	None needed because no HEs were conducted.	Customised severity ratings were introduced for assessments because Nielsen's were deemed insufficient for the SAD.	Customised severity ratings that assess the degree of usability violations with regard to the SAD may need to be introduced.

It must be mentioned that the comparison is limited to studies D and E owing to their systematic approach, which is aligned with the systematic approach proposed in this research. In comparison, the other studies recommended isolated methods for developing heuristics. It should be noted that all methods, excluding the factor analysis method, are integrated into the new three-phase process that is presented in chapter 4.

Despite their drawbacks, HEs still have inherent value and the need to improve upon these remains strong (Law & Hvannberg, 2004). When well planned and with an astute selection of evaluators (in terms of numbers and expertise), HEs are appropriate for directing design iterations (Cockton & Woolrych, 2002). However, their value should not be underestimated as they can identify errors that can be more costly in various contexts (e.g. OHSNs) (Cockton & Woolrych, 2002). An added strength of HEs is that they often yield problems that designers did not consider. It is also stated that there is still a place for reliable UIMs, based on the original rationale for their development, which is to save valuable resources. Eliminating risk and saving time and money are the most appealing virtues that they offer. Therefore, instead of trying to eradicate the use of UIMs, the focus should rather be on how to improve their quality, without increasing costs. They should also have the ability to be applied in more contexts and become more practical and effective.

To our knowledge, no heuristics address the usability limitations specific to the security and privacy of websites/applications. Therefore, guidelines, principles, policies and standards from the security, privacy, usability and USec fields have been considered to develop high-level heuristics for USec assessment. The outcome is a USec HE designed to identify usability problems specific to the security and privacy features of OHSNs. The USec heuristics are presented in chapter 4.

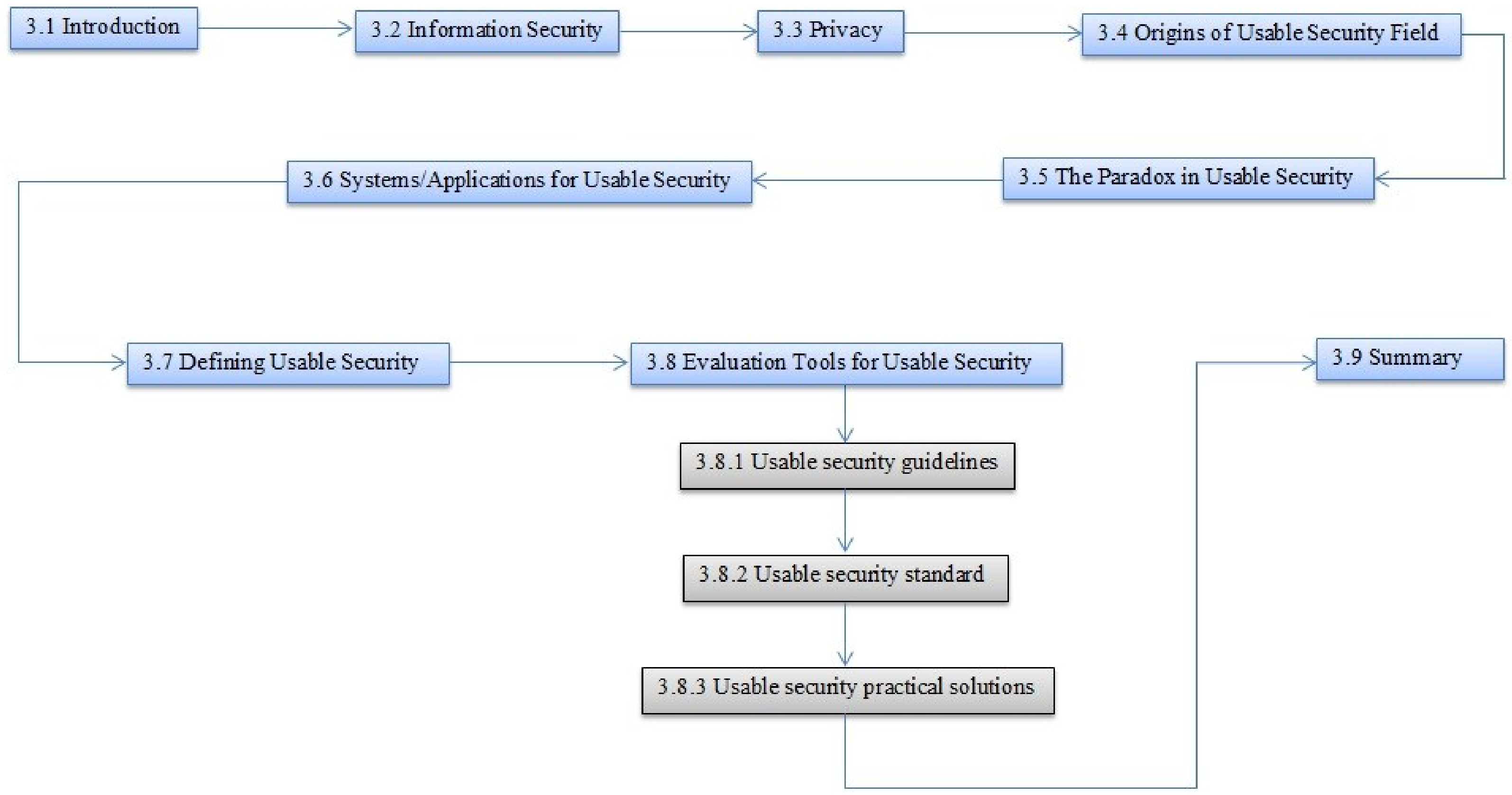
2.7 SUMMARY

This chapter discussed the HCI research field and disciplines. Once HCI had been defined, its characteristics were discussed. These included the human, the machine and the use and context. Following HCI was a discussion on UCD and the fact that the term *HCD* is used interchangeably with UCD and both focus on development, with the user being at the core of design. Consequently, the activities required for HCD were also presented.

Usability is another key discipline in this field. Based on this fact, a discussion on its objectives was provided. Additionally, the usability framework, the model of usability and the principles and guidelines for usability were presented. A discussion on UX, an equally key and relatively new discipline, followed. The UX elements and the UX honeycomb provided a thorough overview of the considerations surrounding UX design. Subsequently, the UXBasis process model was discussed. This model provides an industry perspective for UX design.

The chapter concluded with a discussion on evaluation methods in HCI, which included methods conducted with users, experts or both. In terms of the various UIMs mentioned, HE was the one of particular interest, and therefore discussed in more detail. With regard to the HE UIM, research is currently focused on improving its effectiveness and on the development of new and novel heuristic sets for specialised domains. These areas of research highlight the need of a process that can be applied to develop new heuristics, which is one of the sub-questions that this study will address. In chapter 3 the field of USec is investigated.

LAYOUT OF CHAPTER 3


3.1 Introduction
3.2 Information Security
3.3 Privacy
3.4 Origins of Usable Security Field
3.5 The Paradox in Usable Security
3.6 Systems/Applications for Usable Security
3.7 Defining Usable Security
3.8 Evaluation Tools for Usable Security
3.8.1 Usable security guidelines
3.8.2 Usable security standard
3.8.3 Usable security practical solutions
3.9 Summary

CHAPTER 3: USABLE SECURITY

3.1 INTRODUCTION

This chapter will focus on the field of USec. It is concerned with enhancing the usability and UX of security and privacy features on websites/applications for the intended users. This is a relatively new research field, which requires an understanding of the two fields of information security and HCI. It should be noted that this research study is positioned in the field of HCI. Consequently, it investigates and considers security and privacy as the external field in order to provide the USec HE.

Section 3.2 will introduce the field of information security. Subsequently, privacy is discussed in section 3.3. Section 3.4 explains how the field of USec originated and in section 3.5, the paradox that exists in USec will be discussed. Following this, is a discussion on the types of applications that require USec designs. This is presented in section 3.6. Section 3.7 provides a definition for USec. Existing evaluation tools for USec are mentioned in section 3.8 and the summary is presented in section 3.9.

3.2 INFORMATION SECURITY

A secure application is required to conceal information and resources and to ensure that the data and resources are trustworthy. It should also reassure users that they are able to utilise required information or resources whenever they desire (Rozinov, 2004). Based on this, the three core properties that define information security are confidentiality, integrity and availability (ISO/IEC 27002, 2005; NIST Special Publication 800-53, 2009; ISO/IEC 27799, 2008). An official definition for information security is provided here (ISO/IEC 27002, 2005, p. 1):

> *"InfoSec is the preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved".*

It is widely agreed that security remains a problem domain for UI design. The reason for this is that security has inherent properties (Whitten & Tygar, 2005). These properties need to be considered by developers during design, as they focus on understanding the users and their behaviours, with regard to how they perceive and understand security. These properties include (Whitten & Tygar, 2005; Straub & Baier, 2004; Herzog & Shahmehri, 2007):

- *Users are not motivated to use security because it is usually a secondary goal*. Security is rarely a primary task for the user. Consequently, security features are executed only when needed. Users do not pay attention to them and are unwilling to read manuals relating to their use.
- *Security and privacy policies remain abstract properties that are alien to most users*. It is difficult to find real-world objects that will accurately and intelligibly communicate metaphors for security. This becomes even more difficult in certain security applications, such as Public Key Infrastructure (PKI) and cryptography
- *For effective security management, users require good feedback*. Security should be presented in a faultless manner. Where user intervention is required, the necessary feedback needs to be provided in order for the user to make the correct decision. This feedback needs to be in the user's language and be accurate in terms of accomplishing the task at hand. Failing to understand security messages and features results in the users' privacy being at risk.
- *Unawareness of a security violation*. Immediate consequences for a security violation or insecure behaviour are not always apparent. The effects of such consequences may be long term, while it can also be difficult to link a causative event. Equally, it is also possible that users do not suffer any consequences, despite their insecure behaviours. Therefore, users need to be protected from making any dangerous or irreversible mistakes from the start. This property emphasises that it is difficult for the user to know if the security has been compromised in the case where a mistake or dangerous action took place. Users need to understand the importance of security because they will remain unaware of a possible violation when the system is left unprotected, even for a short time.
- *Guidance for users to ensure that they attend to all aspects of their security*. This is referred to as the "weakest link" property. Security is regarded as a chain and in this chain; it is the weakest link that determines the strength of the whole system. Hence, it is important that all users configure the security settings of an application/website comprehensively (e.g. passwords). All aspects of security need to be attended to as the security of a networked computer is only as strong as its weakened component. If users are to make decisions that are security-critical, they need to make the correct

decisions from their first attempt. Making the correct decisions and correctly configuring the security settings is based on the guidance that is provided to the users via the application/website itself.

Users underestimate the importance of keeping their systems at work and at home secure. In relation to this, Furnell (2005) points out that a compromise of responsibility exists between the developers and users. In certain cases the blame resides with the users because they are using the applications in an irresponsible and careless manner. In other cases, the blame resides with the developers' because they have developed technology with poor usability.

Developers need to consider that users often tend to overlook their security obligations (Furnell, 2004). Developers have gone through great efforts to design suitable and effective security on their software; however, they still depend on the users to use the security features to ensure the security of the system (Furnell, 2004).

As identified in the inherent properties of security, users are not motivated or interested in educating themselves about the security of a software product. Hence, they will only seek this knowledge if a certain situation demands it. Furthermore, they will only take these steps if there is no system administrator to solve their security problems (Furnell, Jusoh & Katsabas, 2006). It is also possible for system administrators to have difficulties with understanding the security of a product. If this can happen, it should not be a surprise that the users are struggling with the security as well (Furnell, 2004).

A major obstacle that prevents users from understanding security options is the language and terminology used to describe them. This is an issue that can be easily overcome with research that can assist developers with regard to security language. Additional help functionality needs to be implemented, as well as training the users in how to address security-related decisions of the product of use (Furnell et al., 2006).

3.3 PRIVACY

Information security was discussed in the previous section. However, it should be added here that another criterion that needs to be considered from the user perspective is privacy. This is the area where different parties collide with regard to information rights, as they have different preferences regarding the flow of information and how it should be utilised (Brunk, 2005). *Privacy* is a difficult term to define because its understanding depends on culture, emotions and technical meanings. One definition is provided by Ackerman and Mainwaring (2005, p. 382):

> *"Privacy is the ability of individuals to control the terms under which their personal information is acquired and used."*

This definition sufficiently describes the types of issues that users will confront during their interactions with applications and websites. Accordingly, they must have the ability to control what they consider to be personal data within a particular social situation. Based on their definition, Ackerman and Mainwaring (2005) identify the following key points about privacy:

- Privacy depends on the information and on the effectiveness of the individuals who control its flow. This point supports the fact that privacy has a natural relationship with concerns in HCI and information security.
- Privacy has similar concerns to security. These are mainly to do with risk, perception and management.
- Privacy is about trust, control and power in social situations. This implies ethical, political and legal issues. Individual freedom and autonomy are expressed through these notions, yet, it is constrained and in certain transactions it can even be a trade-off.

Developing privacy features that are usable requires an iterative design process and testing with users. Only through successive refinement can the developers meet the users' requirements, capabilities and expectations. Usability methods and considerations that can aid this process include the following (Ackerman & Mainwaring, 2005):

- Privacy is not the users' primary task even though it is valued by most. According to Westin, users' privacy concern index can be divided into three distinct categories; fundamentalist, pragmatic and unconcerned (Kumaraguru & Cranor, 2005). Fundamentalists are the most concerned about their privacy, the pragmatic less so, while the unconcerned are generally trustful in providing their personal information. Based on results from a survey conducted on the American public between 1995 and 1999, 25% of the respondents were classified as fundamentalists, 55% as pragmatic and 20% as unconcerned (Kumaraguru & Cranor, 2005).
- Designs need to embrace different types of users with different skills.

- Privacy is critical and, therefore, badly designed features can lead to user rejection and increased development costs.
- Privacy features must respond to the legal and regulatory environment.
- Privacy is contextual. The use of an application's privacy features is based on specifics, such as who the user is, what is privacy being used for, and where, why and when is it being used.

Technology has a strong influence on humans' attitudes towards privacy. This is as a result of the decrease in costs of mass surveillance and data retention technologies. Organisations' desire to collect large amounts of information has increased owing to the affordability. The use of online communication and information is now commonplace. Therefore, it is imperative that users have the ability to control the dissemination of their personal information. One approach is to provide users with technological privacy solutions and tools. These allow users to extend their knowledge in the cyber world and become more aware of the flow of their personal information in this space (Brunk, 2005).

Privacy frameworks have been proposed with the intention to educate and protect individuals. Two examples are the Codes of Fair Information Practice (FIP) and the International Security, Trust and Privacy Alliance (ISTPA) Privacy Framework. The Codes of FIP focus on privacy and ethical data usage. The ISTPA Privacy Framework attempts to build a global alliance for business and technology providers. Its objective is to conduct research and evaluate privacy standards, tools and technologies and to derive new standards for information handling.

The problem with most privacy frameworks is that their design is not based on a user-centred methodology. Brunk (2005) investigated the Codes of FIP, the ISTPA Privacy Framework and Schneier's Security Process Framework in order to develop his own privacy framework; the Privacy Space Framework. By making sense of existing privacy solutions, he could then develop a more user-centred privacy framework. The Privacy Space Framework attempts to classify user experiences as well, in addition to just understanding the features of privacy solutions. Table 3.1 displays the categories, along with their descriptions, that have been are incorporated into the framework (Brunk, 2005).

Table 3.1: Privacy Space Framework (Brunk, 2005)

Category	Description
Awareness	Any type of information that does not require user interaction. These features are informative and help users monitor what is happening. They provide the basis for all privacy-protective behaviours.
Prevention	These features are used as a precaution, such as digital signatures or encryption or secure deletion of electronic documents. However, it is necessary to first have awareness in order to inform users about prevention techniques and current problems.
Detection	These features scan for and actively monitor any potential problems. They usually run in the background, such as in the form of a virus scanner. Information at this stage should provide users with the ability to respond to an identified problem.
Response	This implies taking an action once a problem has been detected, such as blocking networking traffic from certain IP addresses. The violation should then stop.
Recovery	Features that help the user return the system to a normal state, such as patching or restoring to the last good state or reinstalling corrupt files. Response always precedes recovery.

It is useful to consider this framework when attempting to design privacy solutions that users can understand. Much can be gained from the structure of its processes, as these can be applied in the design of privacy features for applications and websites. This framework provides a model for understanding the way users think about privacy solutions.

3.4 ORIGINS OF USABLE SECURITY FIELD

The USec field embraces the fact that most applications have security features that end-users have to interact with. These interactions include configuring security and making security-related decisions. However, the manner in which security aspects are presented, in terms of design and usability, makes it a complicated process, which users prefer to avoid and in most cases even ignore (Furnell et al., 2006).

Reports identify human error as one of the most common causes of security configuration errors. The reason for this is primarily due to the non-usable design of the systems (Furnell et al., 2006; Whitten & Tygar, 2005). A decade of research in the field of USec illustrates that users avoid using complex security mechanisms. Researchers have noted that using security systems that lack usability results in users making mistakes that undermine security (Flechais & Sasse, 2007). It is evident that there is a problem in the interaction between the human element and the technology (design of the interface). This problem relates to the research discipline of HCI as much as it does to the discipline of security. In essence, developing security that is usable has become a necessity.

3.5 THE PARADOX IN USABLE SECURITY

The need to improve the usability of security features is evident, based on previous reports (Furnell et al., 2006; Whitten & Tygar, 2005). However, a paradox exists between security and usability. This paradox has resulted in a debate within the research community about whether these two separate fields can be merged. The majority of researchers believe that this is possible while others disagree (Flechais et al., 2007). Those who disagree state that a trade-off exists; that by improving security, usability is degraded and vice versa (Hertzum, Juul, Jorgensen & Norgaard, 2004).

Several user studies relating to USec have determined the categorisation of different security usability issues. These issues include the following (Muller, 2006):

- Usability problems that do not jeopardise the security of the system.
- Usability problems that position the security of the system at risk. This occurs even though the users have adequate security competence.
- Usability problems that arise as a result of the users' insufficient security knowledge.
- Security problems that are not caused by any user interaction.

Figure 3.1 portrays the area of overlap between security and usability issues in system design. In this figure, one can identify usability issues, security issues and security-critical usability issues. The security-critical usability issues are the area where the overlap between usability and security issues are propagated and where some researchers support the notion that a trade-off exists.

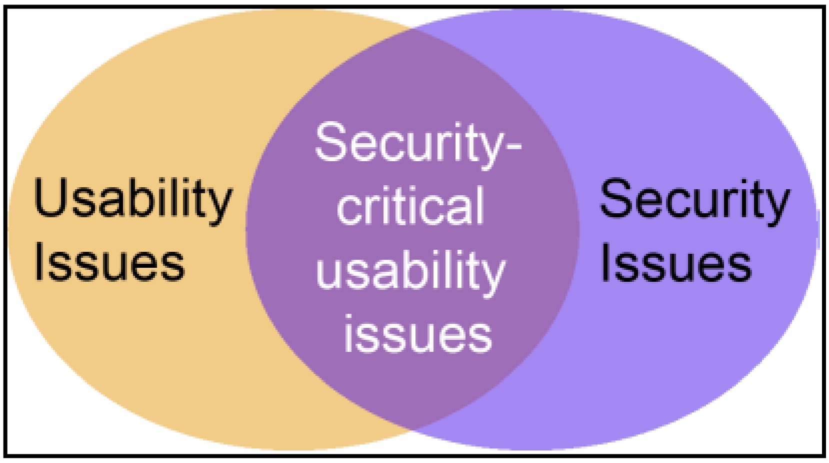


Figure 3.1: The paradox between usability and security issues (Muller, 2006)

Yee (2002, p. 279) is a firm supporter of the idea that usability and security are not at odds with each other. He states his position as follows: "a system that is more secure is more controllable, more reliable and hence more usable; a more usable system reduces confusion and is thus more likely to be secure". In addition, he states that there is a common goal between usability and security advocates, as they both want the computer to carry out the users tasks correctly (Yee, 2002).

An example illustrating the paradox that exists between security and usability is that of the password feature. If the password is based on personal data (e.g. name, date of birth, ID number), usability is enhanced because it is easier to remember. However, there is a risk of a security breach because the password is also weak. Alternatively, using a strong password that combines upper and lower case characters with special characters (e.g. j!8%20C4) improves the security. Yet, it is difficult to remember, thus reducing usability. This becomes even more evident when the user is subscribed to multiple user accounts with different passwords (Hertzum et al., 2004).

It is the users and their passwords that are regarded as the most vulnerable aspect of a secure system. It is clear that a paradox exists: the password must be easy for the user to remember but difficult for another person to guess. Edwards and Petrie (2005) conducted an interesting experiment relating to the memorability and security of passwords. They created five groups of password types, which are presented and described in table 3.2.

Table 3.2: Password classes tested (Edwards & Petrie, 2005)

Group	Class	Description	Examples
1	Random	The eight characters of the password were automatically chosen entirely at random.	ap4AEp£p, djs843nd toc&201!
2	Nonsense	Letters were randomly chosen – but in alternating pairs of vowels and consonants, thereby creating non-words that are to some extent pronounceable.	mejadoro, gitekaba, bekumufi
3	Concatenated pairs	This algorithm constructs a password by concatenating two four-letter words.	rungself, fastlace, banebong
4	Free choice	The user was allowed to choose any eight-character password they wanted.	
5	Guided choice	This was done as in (4), except that the user was given advice on the choice of a good password.	

In order to make the measurement of strength fair, all passwords had to be exactly eight characters long. The results from this experiment showed that the “random” passwords are the most secure but the hardest to remember (only 25% of the participants could remember their passwords). The next most secure was the “guided choice” passwords, which had relatively high memorability rates (81%). “Nonsense” passwords are quite secure but memorability is only at 55%. “Free choice” passwords had high memorability (85%) and were the fourth most secure. “Concatenated pairs” passwords had the lowest levels for security and were fairly memorable (75%) against the rest of the passwords (Edwards & Petrie, 2005). The conclusion was drawn that it is essential for a password to be usable as much as it is secure.

Ideally, security tools (e.g. passwords) should be designed with a 100% strength rate in terms of security and a 100% strength rate in terms of usability. However, this is very difficult to achieve. The important thing is to acknowledge is that both security and usability are equally critical in the design and that the paradox between them can be overcome.

3.6 SYSTEMS/APPLICATIONS FOR USABLE SECURITY

The security tools and features implemented in software are not restricted to the more recognised systems, which are security critical (e.g. antivirus, firewall, operating system etc.). These are embedded in most end-user applications as well (e.g. MS Word, Firefox, MS Outlook etc.) (Furnell, 2005). This emphasises the fact that all users need to be able to understand and effectively configure the security features of the applications they use.

Security in end-user applications may not be equally as critical as those of security applications. However, they do have a level of importance and by making their security features usable, useful practices may be derived. These can then be incorporated into the design of security applications as well. It is also worth considering that most end-users have some type of security application with which they need to interact in order to protect their files and data.

There are a number of potential threats facing end-users today. This alone emphasises the importance of the proper use of security in end-user systems and applications. Yet, a great deal of work still needs to be done in order to make users embrace a security culture. Moreover, the usability of the security tools may be regarded as a significant hurdle in achieving this. Therefore, it is critical that these tools are usable if the users are to benefit from them. In most software, the protection needed is available. Nonetheless, issues such as locating the security features, and understanding and using them effectively are falling considerably short in terms of making these systems usable for the end-user (Furnell, 2005).

The case of security tools being difficult to locate is more prominent in applications where security is not the main purpose (e.g. MS Word). Therefore, security will usually not be transparent to the user. This can potentially lead to a misconception that security is not needed for the specific application (Furnell, 2005).

Users are constantly confronted by security decisions that they need to make when using IT systems. This is largely due to the ever-expanding number of probable threats. These security decisions are not only restricted to specific security tools (e.g. antivirus, firewalls) but also general applications (e.g. MS Word, MS Outlook, and MS Windows). Taking this into account and depending on the context of the software, end-users may be required to configure security-related settings, respond to security-related events and messages, and specify policy and access rights (Furnell, 2007).

Another interesting experiment for USec was conducted on Microsoft's applications Internet Explorer 7 (IE7) and Word 2007 by Furnell (2007). The applications were evaluated against Nielsen's usability heuristics. The purpose of the experiment was to determine usability violations with regard to the security features of both applications. The results are displayed in table 3.3.

Table 3.3: Comparison against Nielsen's usability heuristics (Furnell, 2007, p. 442)

Nielsen Heuristic	IE7	Word 2007
Visibility of system status	Improved attention to the visibility of the security status in comparison to previous versions (e.g. in custom settings; certificate warning bar). Good indications if security has been set low, but no warning in cases where it may be restrictively high.	No status indicators are provided on the main interface to remind the user of security-related aspects (e.g. password protection or Trust Centre settings).
Match between system and the real world	Technical terms still dominate many of the settings and dialogues.	Potential for users not to understand how their actions link to consequent security measures (e.g. setting passwords and encrypting documents).
User control and	Good options for cancelling actions	Some actions within the Document

Nielsen Heuristic	IE7	Word 2007
freedom	within the security settings, and for resetting to defaults.	Inspector cannot be undone.
Consistency and standards	The features considered in this discussion are satisfactory in this respect.	Configuration changes made in the Trust Center are not consistent in scope. There are differences in the password settings depending upon the route used to access them.
Error prevention	The design of the custom settings does not lend itself to prevention of errors, as the available options are not explained.	The presentation of the password options is potentially ambiguous. Users may inadvertently remove important content (e.g. headers and footers) in response to Document Inspector warnings.
Recognition rather than recall	Lack of context-sensitive help means that users may make uninformed decisions.	
Flexibility and efficiency of use	The security related functionality is accessed in the same way, regardless of user ability.	
Aesthetic and minimalist design	If anything, some of the interfaces contain insufficient description, which (combined with the lack of context-sensitive help) potentially leaves users uninformed rather than overloaded with information.	
Help users recognise, diagnose and recover from errors.	Various warning messages have been improved when compared to the previous version. Features are provided to automatically rectify weak security configuration settings.	The Document Inspector allows users to remove elements from their file, but does not offer the option to see exactly what will be removed.
Help and documentation	Absence of context-sensitive help for custom settings. Lack of description for the individual security settings. The potential for available help to be suppressed by "high" security settings.	Several context-sensitive help controls simply link to the top-level Help page. Lack of explicit information (e.g. the scope of Trust Center settings is not explained in several cases).

3.7 DEFINING USABLE SECURITY

The research area of USec is founded on the overlap of two well-established fields in the Information Technology (IT) domain. These fields include HCI and InfoSec. The key focus from the HCI perspective is to consider usability and UX in the design of security and privacy features. Accordingly, the needs of the intended users must be met as this will ensure that the interaction experienced is one of a high quality. The key focus from the InfoSec perspective is to ensure that the security and privacy features do indeed protect the users' information as expected. Properties that define InfoSec, such as confidentiality, privacy, integrity, availability and trust, need to be instilled in the users. Instilling these properties goes beyond the technical capabilities of the product's security; it is also expressed through the design of the security and privacy features that users need to interact with via a UI.

An inspection of the term *USec* will assist in understanding its definition. The two components of this term are "usable" and "security". Therefore, usability is paramount for USec, as it is related to the first component of the term, which is to make the design usable. This is determined by means of users' achieving their goals; hence their satisfaction is a priority (Rogers et al., 2008). Usability is a discipline that originates from the field of HCI, as discussed in chapter 2. Security, which is the second component of the term, is concerned with the technological and managerial procedures applied to systems/applications/websites to ensure that the properties of information security are managed by the application (Rozinov, 2004). Information security was discussed in section 3.2. By introducing the two terms, *usability* and *security*, properties that define USec have been determined. These are based on the cumulative knowledge available in this research field. For an application/website to be usable from a security and privacy perspective, the following is required of the users who are expected to use it (Yee, 2002; Hertzum et al., 2004; Whitten & Tygar, 2005):

1. *Users must be consistently and reliably made aware of the security-related tasks they need to perform.*

2. *Users must be able to easily determine how to accomplish the necessary tasks successfully.*

3. *Users must not be prone to making any dangerous errors.*

4. *Users must be comfortable with the user-interface if they are to continue to use it.*

The properties for USec indicate that the application of use must be secure and the intended users of it must be able to acknowledge the security and privacy vulnerabilities that exist. They can therefore protect themselves by utilising the security and privacy features of the application correctly and effectively because these are easy to use, learn, understand and apply.

3.8 EVALUATION TOOLS FOR USABLE SECURITY

People who are most likely to suffer from "un-USec" are SMEs and domestic users, as they do not have the luxury of ICT support, such as network or system administrators. Nor do they have a help desk as the larger enterprises and organisations usually do (Furnell, 2005). This group of people generally operate without any assistance and are themselves responsible for configuring and protecting their information and resources (Furnell et al., 2006).

It has been determined that there is a need to establish new evaluation methods in order to develop UI architectures for USec. This is determined on the basis of three human characteristics that have been identified among end-users (Muller, 2006). The first characteristic is openness: users want to join or leave the systems at their own will. The second characteristic is adaption: users have their own special requirements, technologies and needs that have to be deployed so that the system continues to evolve. Third is emergence: this relates to adaptation, which leads to new behaviours that have not been seen before. This is a fundamental part of future usability concepts.

Despite the fact that USec is an area of ample interest in the IT community at present, there are limited guidelines, standards or practical solutions that explain how it can be achieved. An interesting argument raised is that users are not the only ones that require USec. Developers have also been identified as a target group that requires USec education and tools (Flechais & Sasse, 2007). Thus, more efforts must be made to ensure that developers are provided with the appropriate development methods to deploy USec in their designs.

Table 3.4 presents an overview of research conducted in an attempt to provide guidelines for USec. The research outputs shown in the table will be discussed in more detail in the subsequent sections. The problematic properties of security were discussed in section 3.2.

Table 3.4: USec literature

Authors	Research output
Whitten & Tygar	Problematic properties of security
Yee	Ten principles for secure interaction design
Johnston, Eloff & Labuschagne	Six criteria for achieving HCI-S (Human Computer Interaction applied in the area of computer Security)
Katsabas, Furnell & Dowland	Ten preliminary guidelines for USec
W3C	Web Security Context: UI Guidelines

3.8.1 Usable Security Guidelines

Various researchers have proposed guidelines for USec. Well-acknowledged and referenced guidelines in the literature include those of Yee (2002), Johnston, Eloff and Labuschagne, 2003 and Katsabas et al. (2005). The works of these researchers provide a foundation on which more evaluation methods for USec can be designed. Accordingly, these were considered in the development of the USec HE, which is presented in chapter 4. Yee's (2002) ten principles for secure interaction design are displayed in table 3.5.

Table 3.5: Ten principles for secure interaction design (Yee, 2002, p. 280)

#	**Principle**	**Description**
1	Path of least resistance	The most natural way to accomplish a task should also be the most secure one.
2	Appropriate boundaries	The UI should expose, and the system should impose distinctions between objects and between actions along boundaries that are relevant to the user.
3	Explicit authorisation	The user's authorities may only be applied to other actors as a result of an explicit user action, which is understood to imply granting.
4	Visibility	The UI should always permit the user to easily check any active actors and authority relationships, which may impact on decisions that are security-related.
5	Revocability	The UI should permit the user to easily revoke previously user-granted authorities, wherever revocation is possible.
6	Expected ability	The UI must never provide the user with the impression that it is possible to complete a specific task that cannot actually be accomplished.
7	Trusted path	The UI needs to provide a trustworthy communication channel for interaction between the user and the entity, which is trusted to manipulate authorities on the user's behalf.
8	Identifiability	The UI must enforce that distinct objects and distinct actions have strictly identifiable and evident representations.
9	Expressiveness	The UI must provide adequate expressive power so that it describes a security policy without unnecessary difficulty and so that users may express security policies in a manner that suits their goals.
10	Clarity	The effects and consequences of any security-relevant action must be clearly apparent to the user before the actual action is taken.

An underlining objective of USec is to reduce the possibility of a user being the weakest link in the system, as discussed in section 3.2. This will largely be achieved by following a UCD process when developing the interface, which needs to guide the user appropriately.

However, in combination with the interface, policies are also needed. These ensure that users are forced to interact with security applications or the security and privacy features of the application of use (Johnston et al., 2003).

HCI applied in the area of computer security (HCI-S) is defined as that part of a UI which is responsible for establishing the common ground between a user and the security features of a system (Johnston et al., 2003). Its purpose is to make the application user-friendly, which will in turn improve its integrity. HCI-S is composed of six criteria that have been developed on the basis of the usability guidelines from Jakob Nielsen. Johnston et al.'s (2003) six criteria for HCI-S are displayed in table 3.6.

Table 3.6: Six criteria for HCI-S (Johnston et al., 2003, p. 678)

#	Criterion	Description
1	Convey features	The interface needs to convey the available security features to the user.
2	Visibility of system status	Users must be able to observe the security status of the internal operations.
3	Learnability	The interface needs to be non-threatening and easy to learn.
4	Aesthetic and minimalist design	Only relevant security information should be displayed.
5	Errors	Error messages need to be detailed and to state and, if necessary, explain where to obtain help.
6	Satisfaction	The interface must help the user to have a satisfactory experience with the system.

The criteria for HCI-S will help build a trust relationship between the user and the interface. Trust is regarded as one of the most essential aspects in a security environment. From the user perspective, an application will only be used to its full potential if the user can trust it. Trust represents the users' belief or willingness to believe the security of the application (Johnston et al., 2003). Users need to trust the system and be assured that security and privacy are available when needed and that they have the ability to both use and understand them without becoming frustrated.

Research has also identified ten preliminary guidelines, which will ensure that developers follow effective and usable presentation methods for security functionality in applications (Katsabas et al., 2005). These are general guidelines that provide developers with considerations and directions for the design of security in their applications. Yet, more efforts are necessary for USec evaluation methods (Flechais et al., 2007). The guidelines are presented in table 3.7 (Katsabas et al., 2005).

Table 3.7: Ten preliminary guidelines for USec (Katsabas et al., 2005)

#	**Guideline**
1	Visible system state and security functions
2	Security should be easily used
3	Suitable for advanced as well as first time users
4	Avoid technical vocabulary or advanced terms
5	Handle errors appropriately
6	Allow customisation without risk of being trapped
7	Easy to setup security settings
8	Suitable security help and documentation
9	Make the user feel protected
10	Security should not reduce performance

Katsabas et al.'s (2005) guidelines are closely related to the key points identified by Furnell et al. (2006) for the usability of security tools. Furnell (2004) mentions two key requirements that need to be considered by the developers. These requirements represent the user as the main component around which security should be built. The first requirement is that the security options have to make sense and the second is that the systems must provide meaningful security-related feedback to the users. Additional key points that extend the two requirements are the following (Furnell et al., 2006):

- *Understandable*. Options and descriptions should speak the "human language". Jargon should be eliminated so that the most novice users are able to use the technologies. It is essential that sufficient help and support is always available.

- *Locatable*. Security features should be easy to find. Where this is not the case it is most likely that users will give up and remain unprotected.
- *Visible*. There should always be indicators (e.g. status indicators, warnings) showing whether security is being applied on the system. This will assist users in applying the appropriate safeguards that were forgotten.
- *Convenient*. The importance of visibility was highlighted; however, it should not be so prominent that it starts to become an inconvenience for the user. If this is the case it is most likely that the user will disable these features.

Apart from the guidelines presented, it is suggested that developers consider USec during the initial stages of design, as they do for usability and security (Balfanz, Durfee, Smetters & Grinter, 2004). This is a major concern because neither security nor usability may be applied to the systems once the primary design work is complete (DiGioia & Dourish, 2005). Making security transparent to the users, designing security user-interfaces that are easy to use and better training for users help promote USec (Brustoloni, 2005; Furnell et al., 2006; Brustoloni, 2006).

Enabling default security on applications is a delicate technique. It ensures that users do not confront any security issues or decisions because it is hidden from them. At the same time, this is not always preferable and is dependent on the specific scenario. Not all default settings can be expected to cater for the security needs of all users. In addition, it is good usability practice to make security transparent. It is vital that security is seen and used, considering the threats available to the user, and it should also be presented in a manner that is intuitive and easy for the user to use. Furnell (2005) questions default security as a technique to promote USec.

3.8.2 Usable Security Standard

The lack of guidance for developers has resulted in the first attempts to provide a USec standard. The first standards effort in this area is provided by the W3C's Web Security Context Working Group (Roessler & Saldhana, 2009). The goal of the standard is to make security usable and to specify user actions for security. The specification is based on known best practices in the area and intends to provide UI guidelines. Most sections assume the audience to contain a certain level of understanding of the core PKI, as applied on the Web. However, there are also sections that do not require thorough PKI knowledge.

The specification addresses potential trust decisions for online users. It extends on this by suggesting ways in which to support them so that users can make safe and informed decisions where possible. To achieve this, recommendations are provided for the presentation of identity information by user agents (e.g. Identity Signal). Recommendations are also provided on how error situations in security protocols can be conveyed. Error-handling recommendations will minimise the trust decisions for users and represent best practices in inducing users towards safe behaviour in circumstances where these decisions must be made. The specification acknowledges the need to communicate context information in a robust manner against attacks, in an attempt to complement decision making. Recommendations are provided for this type of interaction.

The specification states that it is written in a manner that explains the requirements and options for conforming to it as a standard. This structure does not exist for UI guidelines that are not intended to be used as a standard. If the specification is intended to be used as the latter, it can be used as a way to avoid known mistakes in USec.

3.8.3 Usable Security Practical Solutions

There have been some practical applications for USec. Even though these are few, they are a good example of how to improve the usability of security for the user. Hopefully, more USec implementations can follow in the future.

Focus areas for implementing UI design implementations for USec are passwords and logins. User passwords are regarded as the most vulnerable aspect of a secure system. It is difficult to implement usability in them as they need to be easy for the owner to remember, yet difficult for another person to guess. To achieve these conflicting goals new solutions have been proposed and implemented. Several practical solutions for passwords and privacy include:

- *UsableLogin*. Designed by USec Systems and launched in 2009 (http://usable.com/). This is a Web service that allows users to use a simple word (codeword) and combine it with a personal picture for authentication and it provides the user with the ability to log into all websites with one codeword. This codeword will be impossible for anyone else to guess but very easy for the user to remember.
- *Usable PKI*. Designed by PARC (Palo Alto Research Centre), it makes PKI deployment much simpler. It takes the user a total of four easy steps and less than two

minutes to add a new device to the secure wireless corporate network. The original method of deployment took the user about 140 minutes and a total of 38 steps (Balfanz et al., 2004).

- *Click-based graphical passwords*. Most of the best practices referring to USec context information presume visual display (Zurko & Johar, 2008). Also referred to as visual passwords, click-based graphical passwords can be classified into three distinct categories; searchmetric, locimetric and drawmetric systems (Renaud & De Angeli, 2009). Searchmetric systems require users to search a number of images in a challenge set and then select the target images via an input technique. Locimetric systems require users to identify a series of positions within an image and drawmetric systems require users to sketch a drawing (Renaud & De Angeli, 2009). There are a number of examples for each of three categories. PassPoints is an example of a locimetric system. It consists of an ordered sequence of five click-points on an image. In order to login, the user must click within a system-defined region for each click-point. The image is used as a cue to assist the users in remembering their password click-points (Chiasson, Forget, Biddle & Van Oorschot, 2008).
- *Privacy and Identity Management for Europe (PRIME)* (Pettersson, Fischer-Hübner, Danielsson, Nilsson, Bergmann, Clauss, et al., 2005). This research demonstrates the implementation of privacy policies into UI design. The process for the study investigates privacy legislation and then works through derived privacy principles, examines HCI requirements, and concludes with specific design solutions (Patrick & Kenny, 2003). Three alternative UI paradigms for privacy-enhanced identity management are compared, as legal privacy issues derived from the EU directive are mapped onto suggestions of UI solutions. The solutions themselves are grounded in three UI paradigms: a role-centred paradigm, the TownMap-based paradigm and the relationship-centred paradigm (Pettersson et al., 2005). Furthermore, the importance of retaining an individual's right to informational self-determination as a critical element for democracy and society is also emphasised. Once again, the usefulness of their suggested UI solutions depends on the acceptance and application of them by the intended end-users. The point of departure for their UI design solutions is privacy. This is in contrast to this research, where the point of departure is HCI and, in particular, the disciplines of usability and UX. Methods according to which to apply and integrate security and privacy are subsequently considered.

UI design implementations for USec are still limited. However, the existing solutions do provide a foundation for implementing new solutions. Future work in this research could focus on developing UI design implementations for the USec heuristics proposed, based on existing solutions.

A principle that can be considered when creating UI design implementations for the USec checklist items relating to privacy, is the principle of proportionality. This principle originated within the legal and data protection communities and acknowledges that threats to privacy are time, society and culture dependent. The principle states than an application, system, process or tool will need to balance its utility by considering the rights to privacy of the individuals involved. This principle therefore establishes a balance between usefulness and its effects on privacy (Iachello & Abowd, 2005).

Previous research on designing for privacy includes awareness of video-conferencing services, guidelines based on fair information practices (FIPS) to drive privacy-enhanced design and design patterns to privacy problems in ubicom. Expanding on this prior research by attempting to incorporate the principle of proportionality into a design framework resulted in a three-stage method: legitimacy, appropriateness and adequacy, which is displayed in figure 3.2.

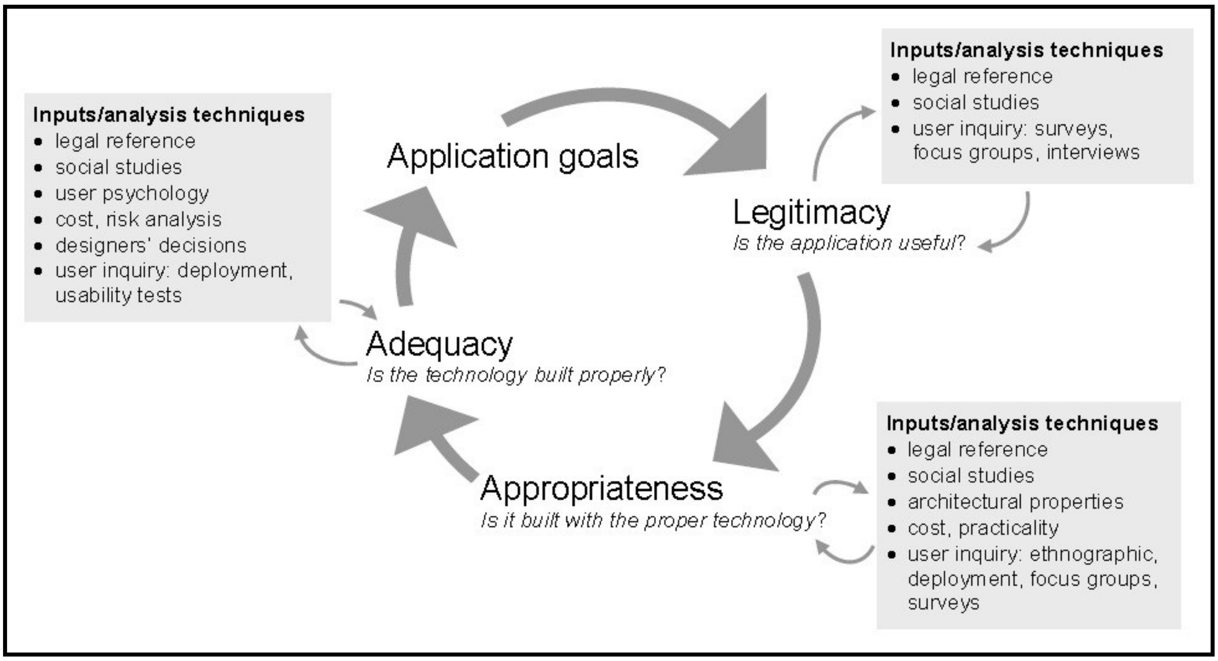

Inputs/analysis techniques
legal reference
social studies
user psychology
cost, risk analysis
designers' decisions
user inquiry: deployment, usability tests
Application goals
Inputs/analysis techniques
legal reference
social studies
user inquiry: surveys, focus groups, interviews
Legitimacy
Is the application useful?
Adequacy
Is the technology built properly?
Appropriateness
Is it built with the proper technology?
Inputs/analysis techniques
legal reference
social studies
architectural properties
cost, practicality
user inquiry: ethnographic, deployment, focus groups, surveys

Figure 3.2: Proportionality design method at a glance (Iachello & Abowd, 2005, p. 93)

The three stages will contribute to achieving the goals of a new application. The legitimacy stage is used to establish whether the application will be useful, while the appropriateness stage determines the best alternative for building the application from a variety of technology solutions and the adequacy stage determines whether the technology is being built properly (Iachello & Abowd, 2005).

Another advantage of the proportionality design method is that it adds minimum overheads to existing user-centred design process models (Iachello & Abowd, 2005). This alone supports its implementation. This design method would be useful when considering the user, context and cultural backgrounds of the intended users of an application. This could then help determine which privacy heuristics are relevant and how they can be applied in design.

A critical factor contributing to research into the implementation of privacy policies and security in UI design is trust. It is essential, if users are to use a system, whether it is e-commerce or a computer program, that it is used to its full potential. User surveys in Europe show that users do not trust network data processing to preserve privacy (Pettersson, & Fischer-Hübner, 2004). Instead, Internet users are concerned about divulging personal information online and are worried that they are being tracked as they use the Internet. Moreover, users are failing to register on www sites because they feel that they cannot trust the Internet with personal or financial information (Kobsa, 2002).

Herzog and Shahmehri (2007) have researched the deployment of USec from a different, yet equally important, perspective. They acknowledge the need for new guidelines and evaluation tools for USec, but nevertheless claim that little has actually been done with regard to how applications may help users in security decisions and tasks. For that reason, they investigate the various help techniques that will better suit users with their security-related tasks. These help techniques include online documentation, context-sensitive help, wizards, assistants, safe staging, social navigation and built-in hidden security.

Security applications should be provided with a combination of built-in security and user help technique(s) (Herzog et al., 2007). In order to determine which help techniques should be used for a specific security application, user questions have been identified. Depending on whether or not the particular user help technique addresses the questions, a decision may be made as to whether it is usable, thereby making it suitable for the users. The question types with an example are provided in table 3.8.

Table 3.8: User questions for determining user help techniques (Herzog et al., 2007)

Question type	**Example**
Informational	What can I do with this application?
Descriptive	What is this? What does this do?
Procedural	How do I do this?
Interpretive	What is happening now? Why did this happen? What does this mean?
Navigational	Where am I? Where have I come from and gone to?
Choice	What can I do now?
Guidance	What should I do now?
History	What have I done?
Motivational	Why should I use this program? How will it benefit me?
Investigative	What else should I know? Did I miss anything?

As with Furnell (2005), Herzog et al. (2007) question the approach of building in security and automating it, as this prevents any user interaction with the security of the system. They also stress that user help is just one component of the overall security application.

3.9 SUMMARY

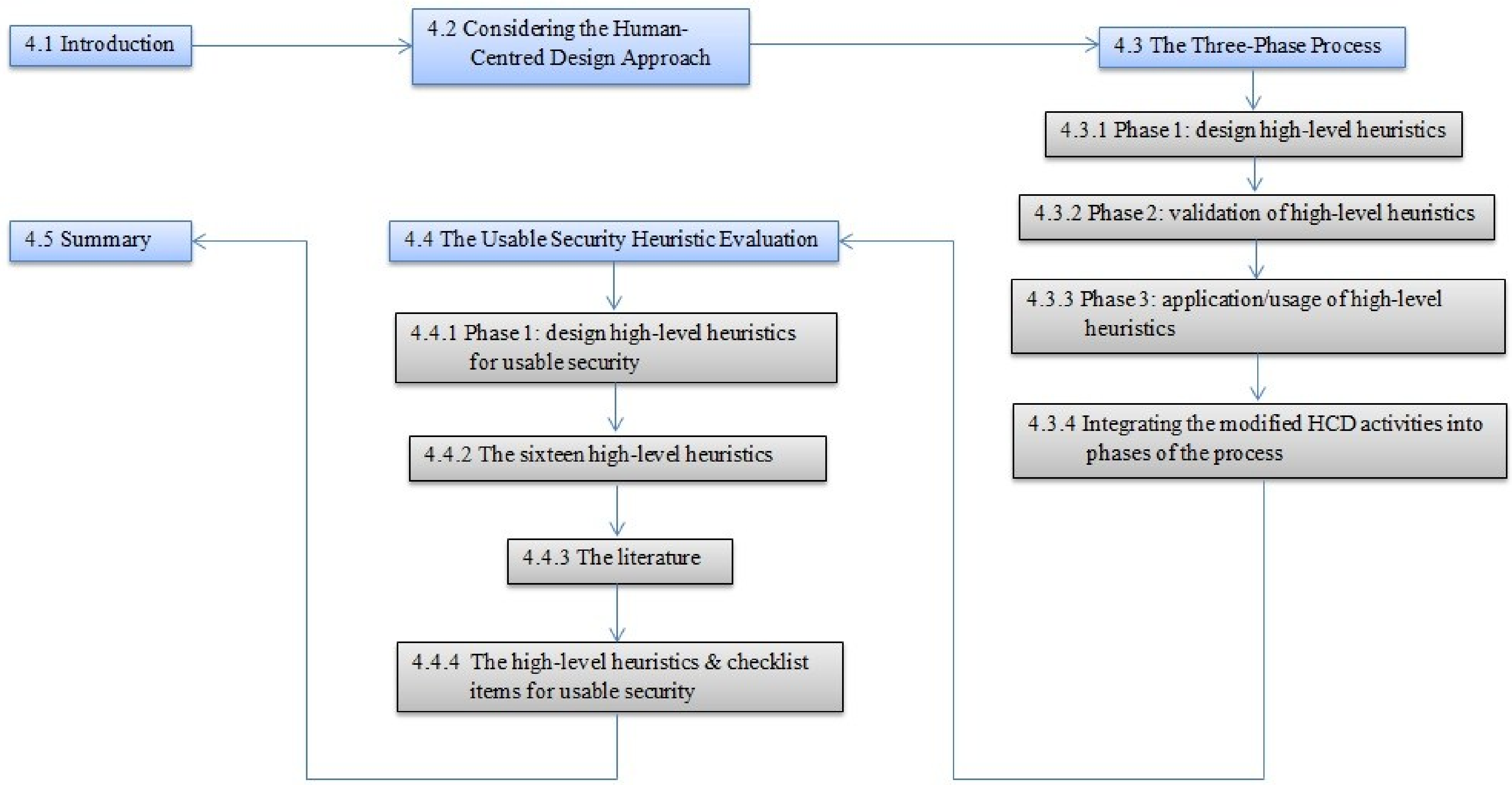
This chapter discussed USec. It pointed out the need to design applications for security that are usable for the respective users. Insight into information security was first provided and the inherent properties of security that make it a difficult domain for UI design were presented. A discussion on privacy and the frameworks that exist for it then followed. Special interest was devoted to the Privacy Space Framework, as it is one of the more user-centred frameworks for privacy available.

A brief overview of how the field of USec originated was then given. This emphasised that the human being is usually the main cause of security errors and breaches. This supplemented the argument that security designs are lacking in terms of usability. Relating to this is the paradox in USec, which was subsequently discussed. This paradox debates whether usability and security can coexist during design. A definition for USec was then provided on the basis of prior research.

The focus then fell on the existing evaluation tools for USec. A decade into this field, the design and evaluation tools for implementing USec solutions in practice are still limited. These are required to assist software developers in their designs. The guidelines that were presented for this included the ten principles for secure interaction design, the six criteria for HCI-S and the ten preliminary guidelines for USec. The first standard in the field, W3C's Web Security Context: UI Guidelines, was also mentioned. In addition, practical solutions for USec were presented, as well as several examples including UsableLogin, Usable PKI, click-based graphical passwords and PRIME.

The need for USec solutions is emphasised in this chapter. However, to provide such solutions it is required that developers are provided with design and evaluation tools for USec. This is addressed by one of the sub-questions in this study, with the development of a HE for USec. In Chapter 4 the process for developing heuristics for a SAD and the USec HE is presented.

LAYOUT OF CHAPTER 4


4.1 Introduction
4.2 Considering the Human-Centred Design Approach
4.3 The Three-Phase Process
4.3.1 Phase 1: design high-level heuristics
4.3.2 Phase 2: validation of high-level heuristics
4.3.3 Phase 3: application/usage of high-level heuristics
4.3.4 Integrating the modified HCD activities into phases of the process
4.4 The Usable Security Heuristic Evaluation
4.4.1 Phase 1: design high-level heuristics for usable security
4.4.2 The sixteen high-level heuristics
4.4.3 The literature
4.4.4 The high-level heuristics & checklist items for usable security
4.5 Summary

CHAPTER 4: THE HEURISTIC EVALUATION DESIGN PROCESS AND THE USABLE SECURITY HEURISTIC EVALUATION

4.1 INTRODUCTION

This chapter will start by presenting a modified version of the human-centred design (HCD) approach. The modified version has a significant contribution to make because it provides a blueprint for the new three-phase process. This process can be applied when developing heuristics for specific application domains (SADs) and is presented and discussed here in detail. Following this, the usable security (USec) heuristic evaluation (HE) will be presented. This is the outcome from phase 1 of the process and includes 13 high-level heuristics for USec and their checklist items.

Section 4.2 will focus on how the original HCD approach has been considered and consequently modified. In section 4.3, the three-phase process to developing heuristics for a SAD is discussed. Following this is the USec HE, which is presented in section 4.4. The summary is presented in section 4.5 and the structure of the chapter is displayed in table 4.1.

4.2 CONSIDERING THE HUMAN-CENTRED DESIGN APPROACH

The HCD approach was introduced in chapter 2 and involves four activities, as presented in section 2.3.1. The approach itself provided a template for the design of a new process to develop heuristics for SADs. The modified HCD approach, which provides the foundation for developing the new process, is displayed in figure 4.1. There are four main reasons why the new process is based on the HCD approach:

1. The new process must provide a purely qualitative approach towards heuristic development, as this will differentiate it from previous attempts.
2. Experts from the SAD have a substantial contribution to make in terms of developing the respective heuristics in the new process.
3. Users can contribute to the design of the heuristics by addressing their concerns, based on their personal experiences, when interacting in the SAD context.
4. The approach determines the types of activities that should be included in the new process to ensure that it follows a qualitative approach and that the approach itself considers the human element (e.g. experts and users) during the development of a new heuristic set.

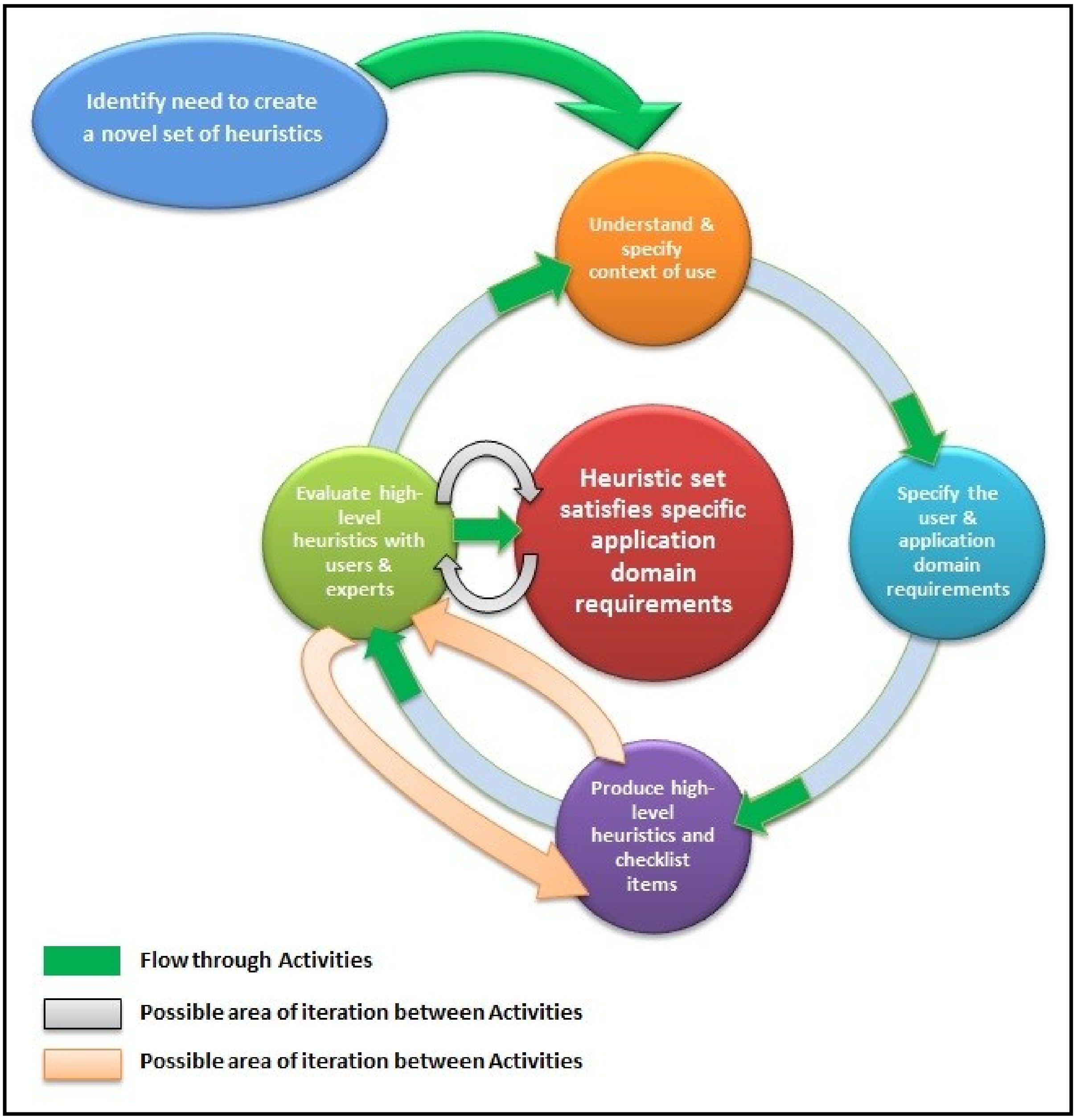

Identify need to create a novel set of heuristics
Understand & specify context of use
Specify the user & application domain requirements
Produce high-level heuristics and checklist items
Evaluate high-level heuristics with users & experts
Heuristic set satisfies specific application domain requirements
🟩 Flow through Activities
▭ Possible area of iteration between Activities
▭ Possible area of iteration between Activities

Figure 4.1: The modified HCD activities for the new process to develop heuristics for SADs

It should be noted that activities in the modified HCD approach correspond to those in the original HCD approach. Similar to the original approach, activities in the modified approach will only initiate once it has been confirmed that there is a need to develop a novel set of heuristics for a SAD. This is confirmed when there are no existing heuristic sets for the SAD or when the sets that do exist are too general and therefore limited in scope to effectively evaluate interfaces in the SAD. Once initiated, the following activities will need to be conducted:

- *Understand and specify the context of use*. Context of use encompasses the characteristics of the intended users who use the application/website and the type of tasks that participants will need to perform to evaluate the applicability of the new heuristic set.

- *Specify the user and application domain requirements*. This activity determines and specifies the major requirements for the new heuristic set. These requirements are dependent on the intended users (includes domain experts), type of application/website and requirements representing the SAD. Identifying the requirements requires a thorough literature review.
- *Produce high-level heuristics and checklist items*. Potential high-level heuristics and checklist items for the SAD are produced as part of this activity. The heuristics are based on themes that emerge from the requirements, which are determined in the previous activity.
- *Evaluate high-level heuristics with users and experts*. User-centred evaluation (from a user and expert perspective) is essential in determining if the new heuristic set is a success. Moreover, new information regarding user requirements may be collected and baselines can be established for modifying heuristics and checklist items. This can provide feedback, which then can also be used to improve the heuristic set to ensure that user and application domain requirements have been fulfilled.

The modified HCD approach concludes when users and experts are satisfied with the new heuristic set ("*Heuristic set satisfies SAD requirements*"). This includes improving the set according to the recommendations and comments that were provided during the evaluations. Iterations will be required between activities to ensure that suggested improvements have been completed, as displayed in figure 4.1. This completes and confirms the transformation from high-level heuristics for the SAD to heuristics for the SAD.

4.3 THE THREE-PHASE PROCESS

In chapter 2, the methods that have been applied in previous research to develop heuristics for a SAD were discussed. These are summarised in table 4.1. A criticism of those methods relates to the validation of the novel heuristics. Additionally, by relying on a single method for developing heuristics, important aspects can be overlooked and a bias can result from the creator of those heuristics (Sim et al., 2009). Researchers have also stressed the need for a tool to create taxonomies of problems within various application contexts. This will result in a selection of more effective and context-specific heuristics (Hvannberg et al., 2007;

Somervell & McCrickard, 2005). In alignment with these views, this research introduces a new three-phase process to create heuristics for a SAD.

Table 4.1: Methods to develop heuristics for a SAD

Heuristic development	Authors/researchers	Methods
Study A	Paddison and Englefield (2004)	1. Literature review 2. Prior studies analysis
Study B	Ling and Salvendy (2005)	1. Literature review 2. Tailored made heuristics 3. Evaluation results
Study C	Nielsen (1994)	1. Factor analysis 2. Explanatory coverage process
Study D	Somervell and McCrickard (2005)	1. Identify system class examples 2. Extract design knowledge 3. Group and label heuristics 4. Derive final heuristics
Study E	Sim et al. (2009)	1. Determine effectiveness of Nielsen's well-known heuristic set 2. Build corpus of usability problems 3. Corpus synthesis into heuristics

The proposed three-phase process is presented in figure 4.2, which highlights the way methods from prior research studies are incorporated into each phase of the new process (Yeratziotis, Pottas & van Greunen, 2011a). Each of the studies along with their methods for heuristic development is displayed. The studies are represented by capital alphabetical letters that match those in table 4.1. The colour of a method corresponds to the colour of the phase in which it is incorporated. All the methods are incorporated into the new process except for Nielsen's factor analysis method, as this is a quantitative method (Nielsen, 1994). The process envisaged in this research is founded on a qualitative approach for heuristic development. In some instances, a method is used in multiple phases of the process. In this case, the outline colour of the method corresponds to the colour of the phase in which it is incorporated with a lower impact degree. The inline colour of the method corresponds to the colour of the phase in which it is incorporated with a higher impact degree.

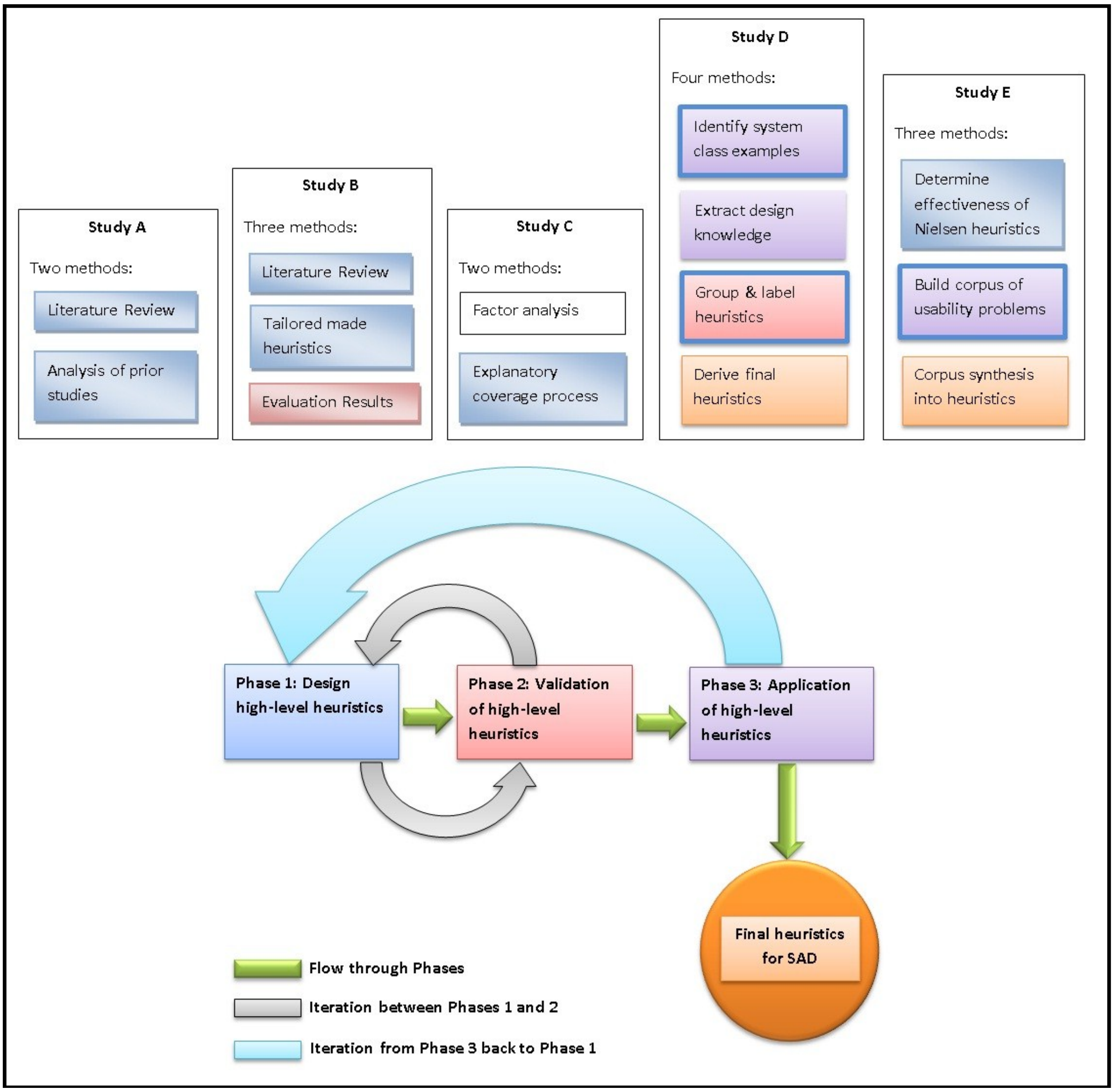

Study A
Two methods:
Literature Review
Analysis of prior studies
Study B
Three methods:
Literature Review
Tailored made heuristics
Evaluation Results
Study C
Two methods:
Factor analysis
Explanatory coverage process
Study D
Four methods:
Identify system class examples
Extract design knowledge
Group & label heuristics
Derive final heuristics
Study E
Three methods:
Determine effectiveness of Nielsen heuristics
Build corpus of usability problems
Corpus synthesis into heuristics
Phase 1: Design high-level heuristics
Phase 2: Validation of high-level heuristics
Phase 3: Application of high-level heuristics
Final heuristics for SAD
Flow through Phases
Iteration between Phases 1 and 2
Iteration from Phase 3 back to Phase 1

Figure 4.2: The three-phase process to develop heuristics for a SAD (Yeratziotis et al., 2011a).

The process initiates in phase 1, where the focus is on designing high-level heuristics for the SAD. Once this is completed the process continues into phase 2. At this point experts will be provided with a validation tool to assess the proposed high-level heuristics. The emphasis here is purely on assessing these heuristics. Once this phase is complete the process continues to the next phase, phase 3, which focuses on applying the high-level heuristics in context (in this research the context is the OHSNs). To achieve this, suitable websites/applications are identified and evaluated with the novel high-level heuristics, as developed in phase 1. These evaluations are conducted by users.

The analysis of phases 2 and 3 will determine the number of iteration cycles that will need to follow and between which phases the iterations need to occur. The iterations are required in order to modify and improve the high-level heuristics according to the experts' and users' recommendations and observations. The revised high-level heuristics will then be re-evaluated by the experts in phase 2, where they will use the same validation tool. Cost and time will determine whether users are required to re-evaluate as well in phase 3. Their recommendations have been provided in the initial evaluation and, at this point, it is the experts' assessments that are more significant, as they have the necessary knowledge and experience to determine if the new high-level heuristics meet the requirements of the SAD. Once the experts are satisfied with the revised high-level heuristics, the process will conclude with a final set of heuristics. This proves acceptance, and the "transformation" of high-level heuristics for a SAD to heuristics for a SAD is therefore confirmed. However, if the experts are unconvinced, the process will need to iterate back to the relevant phases and the high-level heuristics need to be revised accordingly. These modifications are now based on the experts' recommendations from their second round of assessments. This iteration process continues until the experts are satisfied with the suggested improvements to the high-level heuristics.

Figure 4.3 presents a more comprehensive representation of the process. It combines high- and low-level detail regarding the process of developing heuristics for SADs. The high-level representation is based on figure 4.2 and represents the three phases as circles within a funnel. The flow and iteration cycles between the circles has been discussed above in the description of the process. The low-level representation decomposes each of the three phases and displays the tasks that are involved in each of them. A detailed discussion of each phase follows in the subsequent sections.

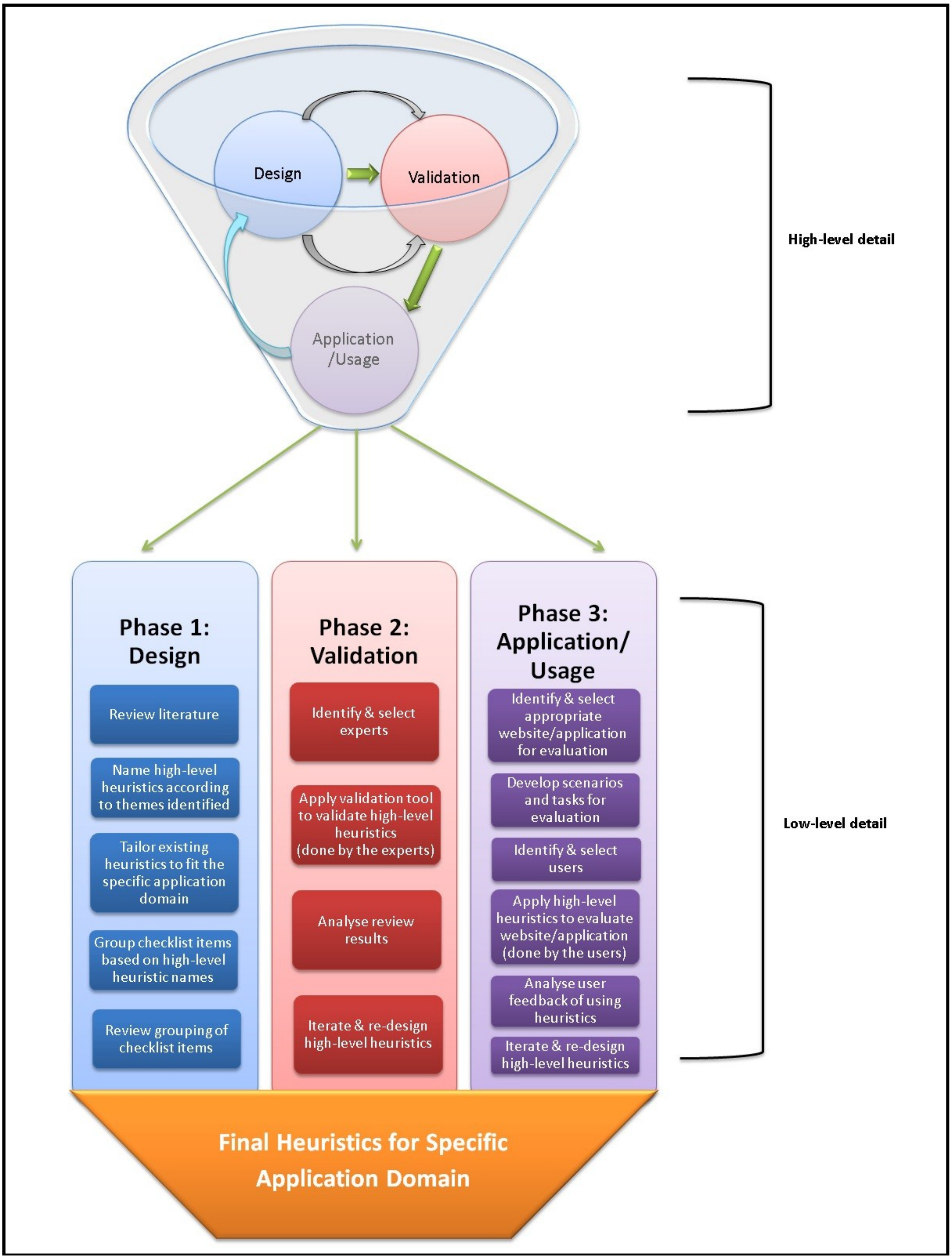

Design
Validation
Application /Usage
High-level detail
Phase 1: Design
Review literature
Name high-level heuristics according to themes identified
Tailor existing heuristics to fit the specific application domain
Group checklist items based on high-level heuristic names
Review grouping of checklist items
Phase 2: Validation
Identify & select experts
Apply validation tool to validate high-level heuristics (done by the experts)
Analyse review results
Iterate & re-design high-level heuristics
Phase 3: Application/ Usage
Identify & select appropriate website/application for evaluation
Develop scenarios and tasks for evaluation
Identify & select users
Apply high-level heuristics to evaluate website/application (done by the users)
Analyse user feedback of using heuristics
Iterate & re-design high-level heuristics
Low-level detail
Final Heuristics for Specific Application Domain

Figure 4.3: High- and low-level detail of the three-phase process to develop heuristics for SADs (Yeratziotis et al., 2011a).

It is important that experts confirm the suitability of the high-level heuristics for the SAD. By acknowledging this, they are ensuring that software developers can use the heuristics to develop more usable user interfaces for the SAD. As a result, users of the intended website/application will benefit, as the overall usability and user experience is enhanced. Simultaneously, developers will also benefit because the probabilities of users accepting their designs are equally enhanced. They therefore become the typical users of it and do not abandon it.

4.3.1 Phase 1: Design High-level Heuristics

Phase 1 consist of five tasks, as displayed in figure 4.4. One will notice that in figure 4.3, phase 1 consists of four tasks. This is because tasks 4 and 5 are separated in figure 4.4, whereas in figure 4.3 they are combined. Section 4.4 will demonstrate how phase 1 was conducted.

Prior research refers to this phase as the meta-analysis approach (Sim et al., 2009). Sources that are used for evidence include guidelines, journal papers or grounded theory based on primary research. However, the issue of credibility and the validity of the data to ensure corpus quality remains a key concern.

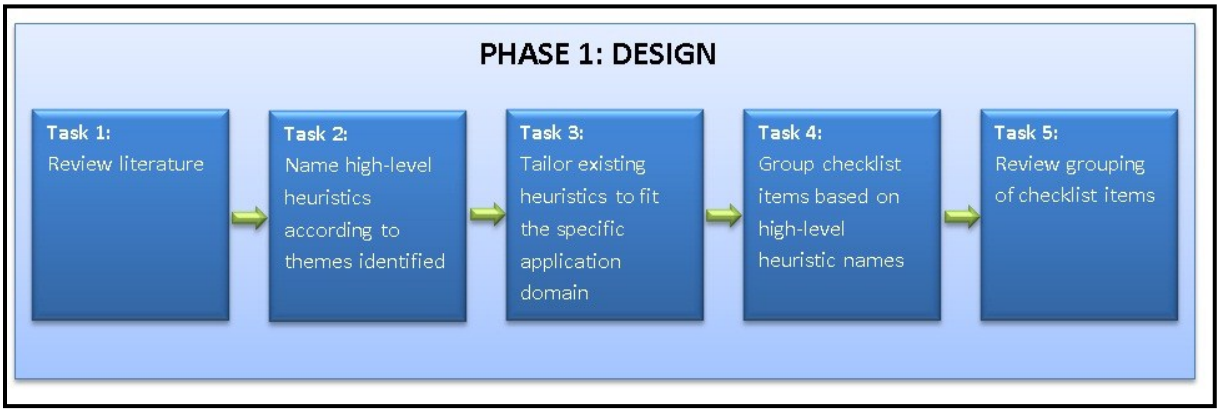

PHASE 1: DESIGN
Task 1: Review literature
Task 2: Name high-level heuristics according to themes identified
Task 3: Tailor existing heuristics to fit the specific application domain
Task 4: Group checklist items based on high-level heuristic names
Task 5: Review grouping of checklist items

Figure 4.4: The five tasks for Phase 1

The five tasks in phase 1 include the following (Yeratziotis et al., 2011a):

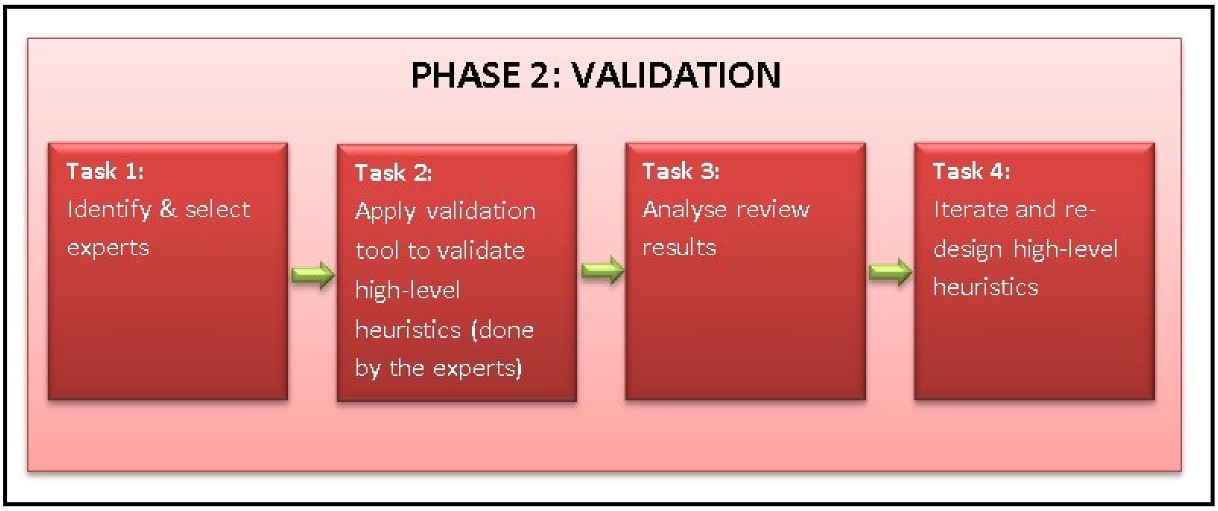
1. *Review literature.* An extensive review of the literature for the SAD must be conducted. For example, in this research study the fields that were investigated include usability, security, privacy and USec. The literature is considered and analysed to determine the requirements that represent each field and to identify the themes that emerge.
2. *Name high-level heuristics according to themes identified.* Wording is implemented to transform the themes into high-level heuristic names with descriptions. These descriptions need to provide a brief understanding of what the themes represent and

address. Existing heuristics need to be referenced in order to understand the level of generality needed in the wording (Sim et al., 2009). This is achieved by applying the tailored made method in the next task. Nevertheless, the new high-level heuristics should not copy existing models too closely and should be specific to the SAD.

3. *Tailor existing heuristics to fit the SAD.* The tailored made method is applied to create checklist items based on the heuristic names. This method is based on modifying existing well-known heuristic sets through the specification of relevant checklist items to address the SAD requirements (Somervell & McCrickard, 2005).
4. *Group checklist items based on high-level heuristic names.* Checklist items that were created when applying the tailored made method are grouped under corresponding high-level heuristics names. This grouping is based on determining which high-level heuristic name better represents the checklist item.
5. *Review grouping of checklist items.* This task focuses on the tool (including all high-level heuristics and checklist items) as a whole, as opposed to task 4, where individual high-level heuristics were populated with checklist items. This implies moving checklist items under a different heuristic name where necessary.

4.3.2 Phase 2: Validation of High-level Heuristics

The issue regarding the credibility and validity of the data to ensure corpus quality is now addressed in phase 2 of the process. Phase 2 consist of four tasks, as displayed in figure 4.5. Section 7.2 will demonstrate how phase 2 is conducted.



PHASE 2: VALIDATION

Task 1: Identify & select experts

Task 2: Apply validation tool to validate high-level heuristics (done by the experts)

Task 3: Analyse review results

Task 4: Iterate and re-design high-level heuristics

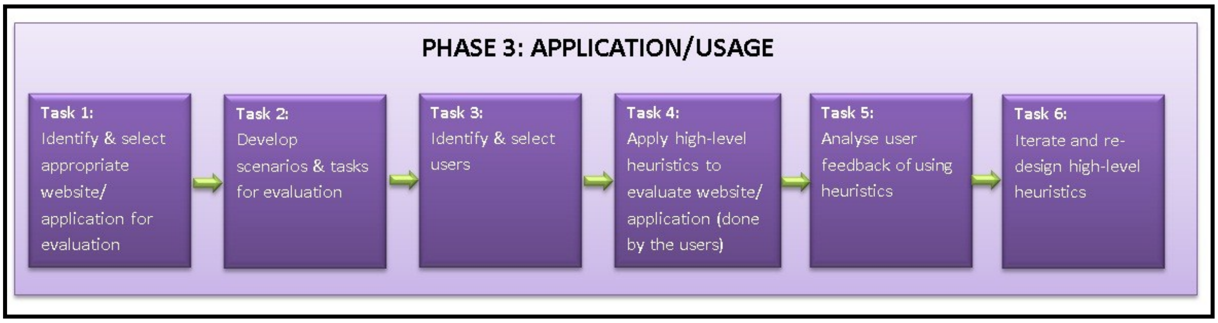
Figure 4.5: The four tasks for phase 2

The four tasks in phase 2 include the following (Yeratziotis et al., 2011a):

1. *Identify and select experts.* It is critical that the most suitable experts conduct the assessments. They need to have the necessary theoretical knowledge and practical experience with regard to the SAD, which ensures that the high-level heuristics address the necessary requirements. For example, experts that will be used to assess the USec heuristics originate from the fields of Security, Usability and USec.
2. *Apply validation tool to validate high-level heuristics.* Experts are provided with a validation tool to assess the high-level heuristics. The validation tool will use rating scales to measure various characteristics of the new HE. These include importance, clarity and completeness of heuristics and checklist items, grouping of checklist items, and ease of application and relevance of new severity ratings. In addition, relevance and novelty of material that was used to formulate the heuristics is also assessed. Other characteristics measured include ease of use, length, effectiveness and quality of the overall HE. All these will have an impact on the adoption of the new heuristics for the SAD.
3. *Analyse review results.* The results from the validations must be analysed. Based on the characteristics that were validated in task 2, it is possible to determine the type of modifications required in order to improve the high-level heuristics in the next iteration cycle.
4. *Iterate and re-design high-level heuristics.* The modifications needed based on the results from task 3 will also determine where iteration is necessary between the phases. For example, if the analysis shows that experts are not satisfied with the relevance of the material used to develop the high-level heuristics, the process will need to iterate back to phase 1. This essentially shows that the requirements for the SAD are not represented within the high-level heuristics. Therefore, all tasks in phase 1 would need to be repeated. In another example, if the analysis shows that the experts are not satisfied with the grouping of the checklist items alone, the process will only need to iterate back to tasks 4 and 5 respectively of phase 1.

4.3.3 Phase 3: Application/Usage of High-level Heuristics

In phase 3, the heuristics must be applied in a context setting. Phase 3 consists of six tasks, as displayed in figure 4.6. It should be noted that the improvements required from the analysis of phase 2 must have been done at this point. Application of the heuristics in context can now proceed. Section 6.3 will demonstrate how phase 3 is conducted


PHASE 3: APPLICATION/USAGE

Task 1: Identify & select appropriate website/ application for evaluation

Task 2: Develop scenarios & tasks for evaluation

Task 3: Identify & select users

Task 4: Apply high-level heuristics to evaluate website/ application (done by the users)

Task 5: Analyse user feedback of using heuristics

Task 6: Iterate and re-design high-level heuristics

Figure 4.6: The six tasks for phase 3

The six tasks in phase 3 include the following (Yeratziotis et al., 2011a):

1. *Identify and select appropriate website/application for evaluation.* As with the previous phase where appropriate experts needed to be identified, the same applies in this task. However, at this point the focus is on identifying appropriate websites/applications for the SAD. Accordingly, the new high-level heuristics must be applied to the selected websites to determine their applicability. This entails determining whether the high-level heuristics serve their intended purpose, which is to detect usability violations with regard to the SAD. Identifying websites for the SAD is generally straightforward. For example, if heuristics are being developed to assess the usability of security and privacy features on banking websites, the context will be e-banking websites. However, cases do exist where selection is more complicated, as was the case for this research study. The high-level heuristics created will evaluate the usability of security and privacy features on OHSNs. A plethora of OHSNs exist; however, not all provide social network capabilities. Therefore, a selection procedure was required to determine the websites that would be used in this research study.
2. *Develop scenarios and tasks for the evaluation.* Scenarios and tasks must be identified at this point. These will be executed during formative usability evaluation sessions and are tasks that typical users will experience during their interaction with the website/application. Scenarios will help formulate a mental model for the users during the evaluation. The tasks that the users will undertake must demonstrate the applicability of the new high-level heuristics. For example, for this research study the heuristics developed examine the usability of security and privacy features of OHSNs. Therefore, all tasks will relate to the security and privacy of the website.
3. *Identify and select users.* Once the scenarios and tasks have been developed for the formative usability evaluations, users will need to be selected. There are no criteria for selecting the users. Preferably, one would approach potential users of the

website/application. For this research study, six postgraduate students from the fields of usability and UX, InfoSec and health informatics conducted the user testing.

4. *Apply high-level heuristics to evaluate the website/application.* While users are progressing through the scenarios and conducting the related tasks they become more familiar with their environment and continue to develop their mental model. They also start developing experiences during their interactions. This provides them with a foundation of knowledge which helps them to better understand the high-level heuristics and checklist items (developed in phase 1), which will be applied to examine the website/application. For example, in this study users will be conducting security and privacy tasks and during the course of this will identify usability issues (if they do exist) through their experiences. By applying the new heuristics and checklist items they will determine if their usability concerns have been addressed. Once the users have completed the tasks and applied the high-level heuristics to evaluate the website, they will complete a user satisfaction questionnaire. The questionnaire focuses on their overall experience and recommendations regarding the application/usage of the new high-level heuristics and their checklist items.
5. *Analyse user feedback of using heuristics.* The results from the evaluations must be analysed. Based on the results, it is possible to determine the types of modification required in order to improve the high-level heuristics.
6. *Iterate and re-design high-level heuristics.* As with this task in phase 2, the modifications needed are based on the results, which will also determine where iteration is necessary between the phases.

4.3.4 Integrating the Modified HCD Activities into Phases of the Process

The modified HCD activities and the three phases of the new process have been introduced. Accordingly, it is required that the modified HCD activities be incorporated into the new three-phase process. This ensures that the approach envisaged for heuristic development can be achieved based on the reasons mentioned in section 4.2. It should also be noted that there are four activities in the modified HCD approach, while there are only three phases in the new process.

It is important to state that the purpose of the HCD approach and, consequently, the modified HCD approach, is to identify the types of activity that should be incorporated into the new process to ensure that it is a human-centred process. Consequently, all modified activities have been considered in the process and are represented as tasks within a phase. Figure 4.7 displays the phases in which the modified HCD activities are considered.

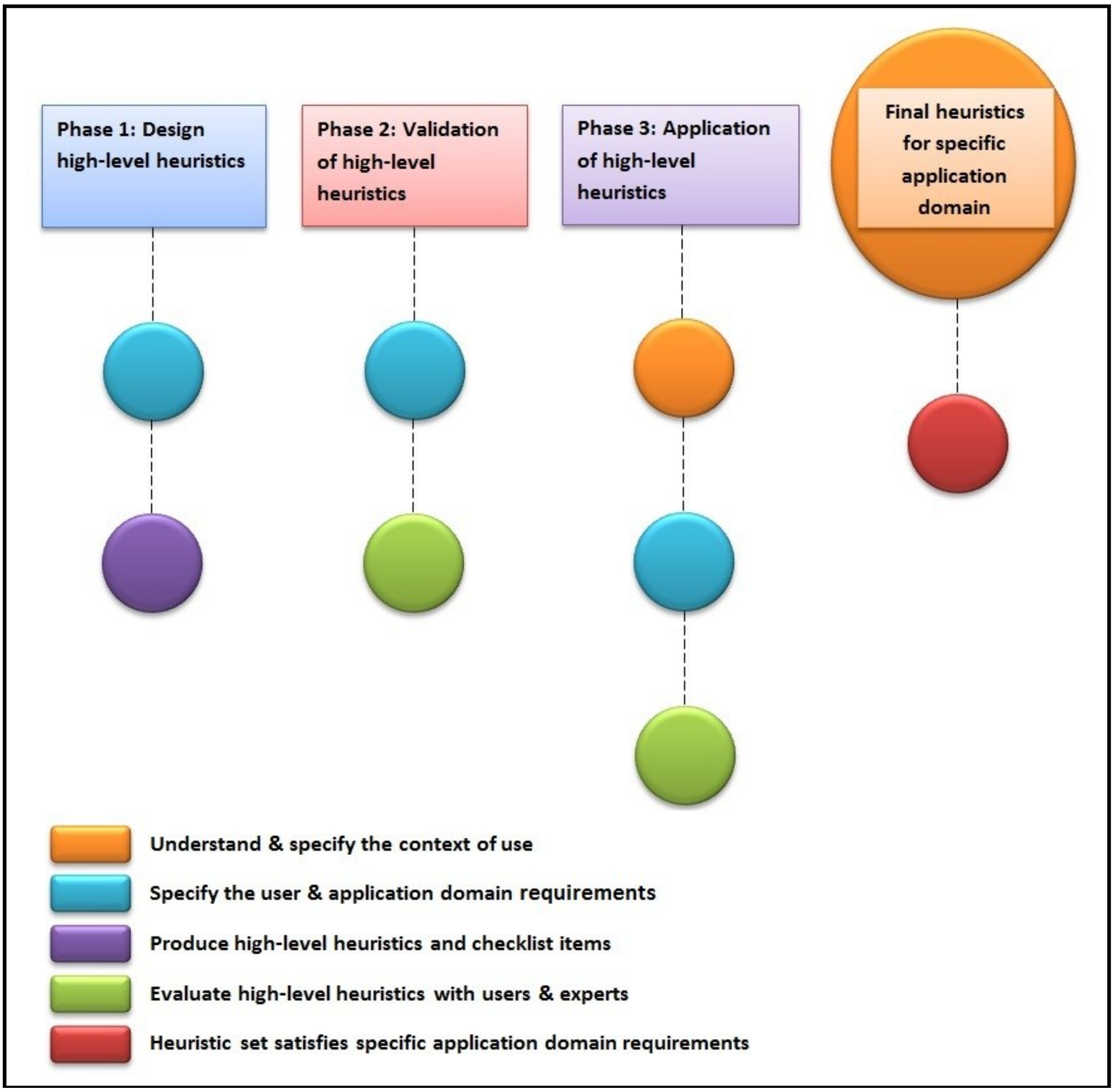

Phase 1: Design high-level heuristics
Phase 2: Validation of high-level heuristics
Phase 3: Application of high-level heuristics
Final heuristics for specific application domain
Understand & specify the context of use
Specify the user & application domain requirements
Produce high-level heuristics and checklist items
Evaluate high-level heuristics with users & experts
Heuristic set satisfies specific application domain requirements

Figure 4.7: Occurrence and correspondence of HCD activities in the new process to develop heuristics for SADs

In figure 4.7 it is noteworthy that an activity from the modified HCD approach can be incorporated into multiple phases of the process. In essence, the figure illustrates an occurrence of an activity within a specific phase or a correspondence between an activity and a phase from the process. Firstly, there is a need to create a novel set of heuristics. Once confirmed, based on figure 4.7, the following apply:

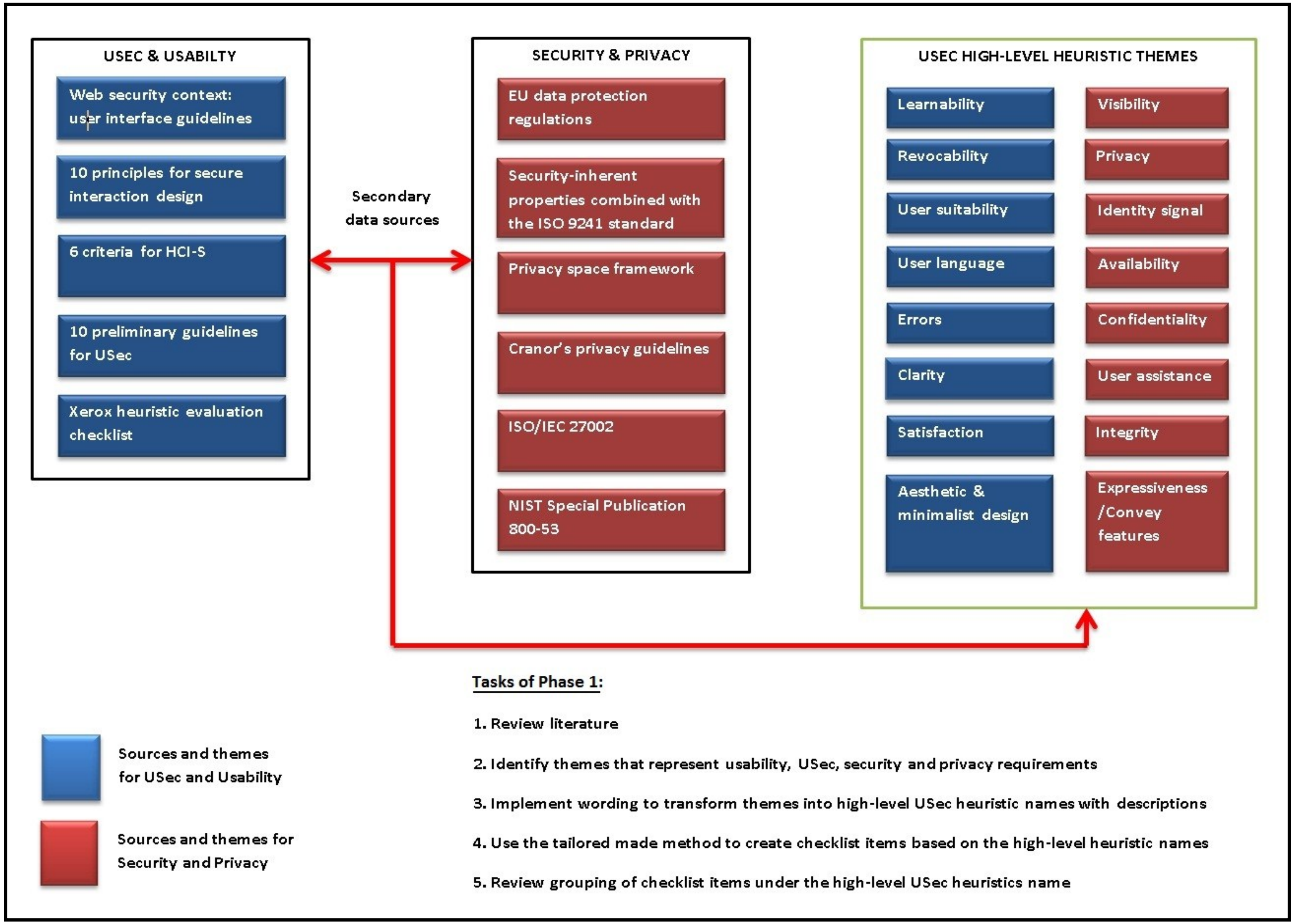
- Phase 1: Design high-level heuristics – In phase 1 there are occurrences of the modified HCD activities “*Specify the user & application domain requirements*” and “*Produce high-level heuristics and checklist items*”.
- Phase 2: Validation of high-level heuristics – In phase 2 there are occurrences of the modified HCD activities “*Specify the user & application domain requirements*” and “*Evaluate high-level heuristics with users & experts*”.
- Phase 3: Application of high-level heuristics – In phase 3 there are occurrences of the modified HCD activities “*Understand & specify the context of use*”, “*Specify the user & application domain requirements*” and “*Evaluate high-level heuristics with users & experts*”.
- Final heuristics for SAD – Correspondence with modified HCD activity “*Heuristic set satisfies application domain requirements*”.

4.4 THE USABLE SECURITY HEURISTIC EVALUATION

This section discusses the development of the USec high-level heuristics and their checklist items. It is based on phase 1, *Design high-level heuristics*, from the three-phase process to develop heuristics for a SAD. The tasks that are conducted in phases 2 and 3 of the process will be discussed in more detail in chapters 6 and 7.

4.4.1 Phase 1: Design High-level Heuristics for Usable Security

Phase 1 is based on five tasks, which are presented in figure 4.8. The figure also displays the literature that was considered for the development of the high-level heuristics and the themes that emerged from it. Figure 4.8 illustrates how the USec and usability guidelines and security and privacy standards contributed to the USec high-level heuristic themes using colour-coding.



USEC & USABILTY

- Web security context: user interface guidelines
- 10 principles for secure interaction design
- 6 criteria for HCI-S
- 10 preliminary guidelines for USec
- Xerox heuristic evaluation checklist

Secondary data sources

SECURITY & PRIVACY

- EU data protection regulations
- Security-inherent properties combined with the ISO 9241 standard
- Privacy space framework
- Cranor's privacy guidelines
- ISO/IEC 27002
- NIST Special Publication 800-53

USEC HIGH-LEVEL HEURISTIC THEMES

Learnability	Visibility
Revocability	Privacy
User suitability	Identity signal
User language	Availability
Errors	Confidentiality
Clarity	User assistance
Satisfaction	Integrity
Aesthetic & minimalist design	Expressiveness /Convey features

Tasks of Phase 1:

1. Review literature
2. Identify themes that represent usability, USec, security and privacy requirements
3. Implement wording to transform themes into high-level USec heuristic names with descriptions
4. Use the tailored made method to create checklist items based on the high-level heuristic names
5. Review grouping of checklist items under the high-level USec heuristics name

🟦 Sources and themes for USec and Usability

🟥 Sources and themes for Security and Privacy

Figure 4.8: Phase 1: Design high-level heuristics

The five tasks that were followed to design the high-level heuristics for USec include:

1. Conduct a literature review in the fields of usability, UX, USec, security and privacy to identify relevant secondary data sources. In this study, the secondary data focuses on four sets of USec guidelines, the Xerox HE checklist and six security and privacy guidelines and standards that are subsequently discussed. The USec guidelines include the following:
    - *Web security context. User Interface Guidelines of the W3C* (Roessler & Saldhana, 2009) – The purpose of the specification is to define requirements and guidelines for Web security context in-formation. Its focus is on the communication and presentation of such information to users.
    - *Ten principles for secure interaction design* (Yee, 2002) – The paper describes the use of a model for secure interaction design and suggests ten principles.
    - *Six criteria to achieve Human Computer Interaction applied in the area of computer Security (HCI-S)* (Johnston et al., 2003) – The paper attempts to promote and enable security awareness for users that interact with computer systems. It uses criteria for successful HCI within a security specific environment.
    - *Ten preliminary guidelines for USec* (Katsabas et al., 2005) – The paper describes the use of standard HCI principles to develop ten guidelines that support the inclusion of security features within applications.
    - *Xerox HE checklist* (Pierotti, 1995) – A popular HE that contains sets of checklist items for assessing the usability of a system. Moreover, it helps achieve usability because it operationalises Nielsen's widely accepted heuristics for usability (Ballard, 2010).

    The following security and privacy standards and guidelines were considered:

    - *EU data protection regulations* (Centre for Democracy and Technology, 2009) - The EU Directive incorporates the seven principles of the Organization for Economic Cooperation and Development (OECD), which relates to the privacy of personal records. It forms legislation for EU countries.
    - *Security-inherent properties combined with ISO (International Organization for Standardization) 9241* (*Ergonomic requirements for office work with visual display terminals)* (Straub & Baier, 2004) – These properties need to be considered by developers during implementation. They focus on

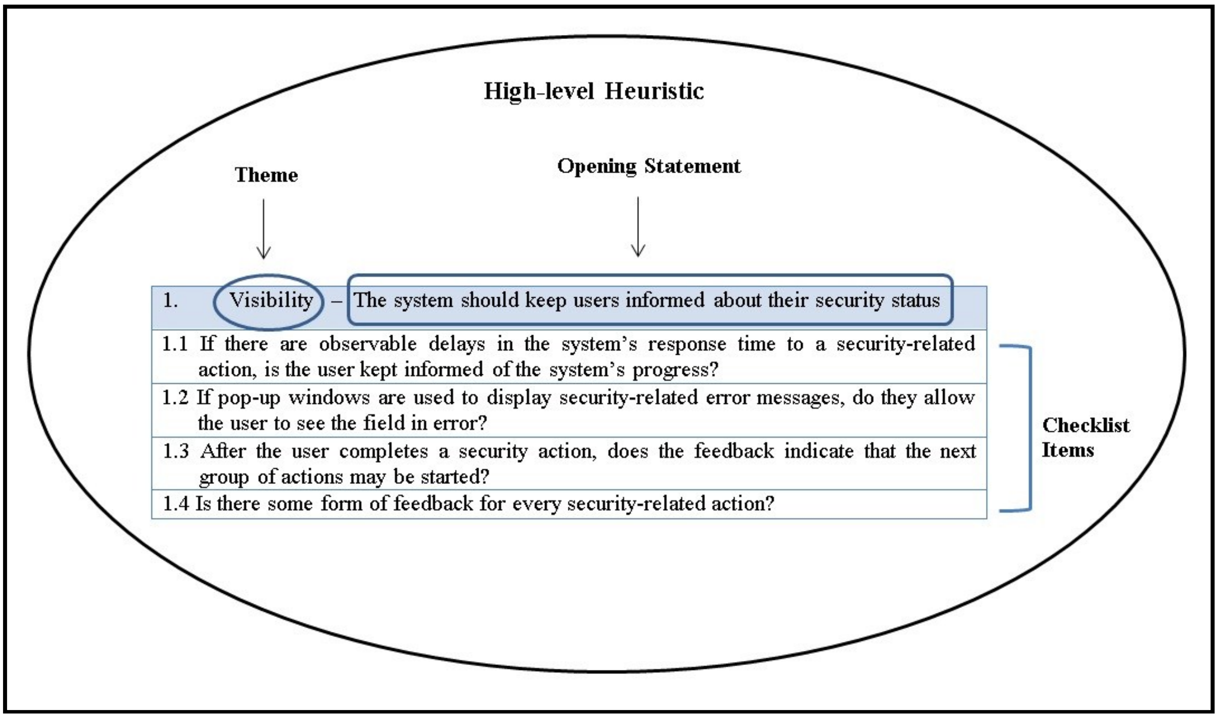
understanding users and their behaviour when interacting with security. These are considered in combination with selected principles from the ISO 9241 standard – specifically, Part 10 of the standard; Dialog Principles.

- *Privacy space framework* (Brunk, 2005) – This is one of the more user-centred frameworks for privacy. In addition to understanding the features of privacy solutions, it attempts to classify the users' experiences. This user-centred approach derives from the inclusion of the "awareness" stage into the framework.
- *Privacy guidelines of Cranor* (Cranor, 2005) – These privacy guidelines attempt to assist software developers with their designs.
- *ISO/IEC 27002 (Information technology — Security techniques — Code of practice for information security management)* (ISO/IEC 27002, 2005) – This document contains guidelines for achieving integrity, confidentiality and availability.
- *National Institute of Standards and Technology (NIST) Special Publication 800-53 (Information Security)* (NIST Special Publication 800-53, 2009) – The document provides recommended security controls for federal information systems and organisations. It was valuable in determining confidentiality, integrity and availability concerns.

The literature selected for the review may raise concerns regarding relevance. This refers to whether the correct literature was selected and why other literature was excluded from the selection. The belief is that the literature selected adequately represents the research fields. This is validated in phase 2 of the process to develop heuristics for SADs, as shown in figure 4.1.

1. Using the literature identified in task 1, identify broad themes that are representative of usability, security, privacy and USec requirements. For example, Yee (2002), Katsabas et al. (2005), and Pierotti (1995) emphasise easy-to-learn applications as a requirement for usability.
2. Implement wording to transform the themes into high-level USec heuristic names with descriptions. These descriptions need to provide a brief understanding of what the themes represent and address. Figure 4.9 provides an example of a novel high-level heuristic from the USec HE. It illustrates the resulting components based on completing the tasks described above. The high-level heuristic consists

of a representative theme (heuristic name) and opening statement (description), followed by several supporting and specifying high-level design issues (checklist items). These assist the experts to understand the application of the heuristic in context. The wording applied to the checklist items of the USec high-level heuristics is based on security, privacy and usability terminologies and requirements.



1.	Visibility – The system should keep users informed about their security status
1.1	If there are observable delays in the system's response time to a security-related action, is the user kept informed of the system's progress?
1.2	If pop-up windows are used to display security-related error messages, do they allow the user to see the field in error?
1.3	After the user completes a security action, does the feedback indicate that the next group of actions may be started?
1.4	Is there some form of feedback for every security-related action?

Figure 4.9: The components of a USec high-level heuristic

It should be noted that novel heuristic names and descriptions have been formulated from the selected literature, yet are still based on the literature. For example, the requirement for "easy to learn applications" is represented in the sources as "Identifiability" (Yee, 2002), "Security should be easily used" (Katsabas et al., 2005) and "Match between system and the real world" (Pierotti, 1995). After applying transformative wording, the requirement is represented in the USec HE as "Learnability – The security features must be easy to learn and to remember how to use them. This implies ease of use". An initial set of sixteen high-level heuristics emerged. These are discussed in more detail in the next section.

3. Use the tailored made method (Ling & Salvendy, 2005) to create checklist items based on the heuristic names. The tailored made method is based on modifying

existing heuristics through the specification of relevant checklist items to address the SAD requirements. This is one of the more common methods applied when developing heuristics (Ling & Salvendy, 2005). The Xerox HE checklist provides a platform for creating the tailored made heuristics through the provision of possible checklist items. Centred on the themes of the USec high-level heuristics, it is possible to identify checklist items from the Xerox HE list that can be tailored to meet the security and privacy requirements identified in task 2. This resulted in the formulation of checklist items for the high-level heuristics for USec. These are discussed in section 4.4.4.

4. Review the grouping of checklist items under high-level USec heuristic names. The focus in this task is on the USec HE tool as a whole, as opposed to task 4, where individual high-level heuristics were populated with checklist items. This implies moving checklist items under a different heuristic name where necessary. A relevant example is provided in the next section.

4.4.2 The Sixteen High-level Heuristics

The result from following the tasks of phase 1 is 16 high-level heuristics that help examine USec on a website. The high-level heuristics are presented in table 4.2.

Table 4.2: The high-level heuristics for USec

#	Heuristic name	Heuristic description
1	Visibility	Users should be able to observe the security status of the internal operations, so that they always feel a sense of protection.
2	Revocability	Users should be able to revoke actions that they previously granted, if they wish to do so.
3	Clarity	The effects and consequences of any security-related actions must be clearly apparent to the users before the action is actually taken.
4	Expressiveness/Convey features	The users should be guided on security matters, yet at the same time need to have the freedom to express their security ideas and actions.
5	Learnability	The security features must be easy to learn and to remember how to use them. This implies ease of use.
6	Aesthetic and minimalist design	Only the relevant security information should be displayed to the users.
7	Errors	The error messages need to be detailed and focused on the exact point of error. Information on where to get additional help, if needed, should be provided.
8	Satisfaction	Users should have a satisfactory experience when using the security tools. Security should not reduce performance or irritate users by interfering with their tasks.

#	Heuristic name	Heuristic description
9	User suitability	Users should have the option for an advanced- or novice-level security interface. This would entail easy customisation of security options and easy setup of security settings.
10	User language	The use of technical and advanced vocabulary should be avoided. This applies to the error messages as well.
11	User assistance	Security help and documentation must be available and easy to locate, when needed.
12	Identity signal	Information regarding the identity of a Website that users may be interacting with should always be provided.
13	Privacy	Users' rights to privacy must be protected. It is necessary to ensure that informational consent practices are followed.
14	Integrity	The system will need to reduce the chance of users making mistakes (e.g. limit the areas where they enter data input manually into fields).
15	Availability	The system needs to be constantly available. It needs to be capable of evaluating whether users have the necessary information to use the system optimally.
16	Confidentiality	Users' personal or private information should be protected.

Although 16 heuristics were initially identified, the final set of heuristics comprises a total of 13 high-level heuristics, each with its own associated checklist items. The decrease in heuristics from 16 to 13 is due to the fact that the Privacy, Availability, Integrity and Confidentiality high-level heuristics are integrated into a single high-level heuristic in the HE, called Security and Privacy. This is because the natural tendencies of the properties overlap and became evident when formulating the checklist items for the heuristics during task 5 of phase 1. For example, to determine whether a checklist item should be grouped under the Integrity or Availability high-level heuristic is not always obvious because it is possible that it meets both requirements. Additionally, if the high-level heuristics were not integrated, they would have been rightly open for criticism. The intention is not to define checklist items for security properties but rather to provide a set of high-level USec heuristics that will assist software developers to improve their designs for security and privacy by considering the users. Therefore, it does not make practical sense to separate these properties but rather to combine them under the collective heuristic of Security and Privacy.

4.4.3 The Literature

A critical factor of the HE is that the heuristics meet the criteria of both security and usability experts alike. Therefore, each high-level heuristic needs to maintain usability and security requirements. It is important to note that each high-level heuristic tests a security/privacy element for its usability. The heuristics do not test the security and usability of the elements as separate entities, but rather test both aspects as one unified entity. The literature used as a foundation to create the high-level heuristic themes is subsequently discussed with a view to showing adequate representation of the usability and USec and security and privacy fields.

Usability and Usable Security

The achievement of usability is essential when developing USec solutions. Hence, the literature selected for the USec field attempts to adhere to this from a usability perspective in an information security application domain. To reiterate, usability is defined as "the extent to which a system, product or service can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use" (ISO 9241-210, 2010).

In this research, usability needs to ensure that users can effectively complete their security and privacy tasks in a manner that does not frustrate them but provides them with a feeling of satisfaction. Widely accepted criteria within the HCI field have been reflected upon to achieve this (Molich & Nielsen, 1990; Nielsen, 1994; Pierotti, 1995). These have consequently been acknowledged and typified within the themes for the USec high-level heuristics. Accordingly, eight of the 16 USec high-level heuristics from table 4.3 and figure 4.8 originate from the usability and USec literature. These are learnability, revocability, user suitability, user language, errors, clarity, satisfaction, and aesthetic and minimalist design.

Security and Privacy

The idea behind the literature selected for this field is that it should help extract the requirements and expectations for the users' security and privacy concerns. This is difficult because most security and privacy standards are focused at the organisational perspective. Therefore, they are concerned with applying security and privacy standards within an organisational structure. This structure does, however, not exist in OHSNs. Nevertheless, a set of well-recognised security and privacy standards were selected. It is not an aim of this research to conduct an extensive analysis and comparison of the security and privacy standards and it should be noted that all standards tend to focus on the same issues and, therefore, information becomes repeatable at some point. Within the selected standards, aspects were identified that would contribute to the formulation of the high-level USec heuristics. Accordingly, a range of well-acknowledged security and privacy standards and models was identified. These include:

- Health Information Trust Alliance (HITRUST) (http://www.hitrustalliance.net)
- Health Insurance Portability and Accountability Act (HIPAA) (AICPA, 2005)
- Generally Accepted Privacy Principles (GAPP) (AICPA, 2005)
- Australia's Privacy Act (AICPA, 2005)
- Canada Personal Information Protection and Electronic Documents Act (PIPEDA) (AICPA, 2005)
- EU Directive (AICPA, 2005)
- OECD guidelines (Centre for Democracy and Technology, 2009)
- US Fair Information Practices in the Electronic Marketplace (FTC) (AICPA, 2005)
- US Safe Harbor (AICPA, 2005)
- Privacy Maturity Model (PMM) (IAPP, 2011)
- US Gramm-Leach-Bliley Act (GLBA) (AICPA, 2005)

Other renowned institutions that publish standards, including security and privacy standards are

- ISO (http://www.iso.org/iso/home.html)
- NIST (http://www.nist.gov/index.html)

As previously stated, the connection between all these standards is that they focus on the business perspective and the organisation (AICPA, 2009). In addition, they all tend to focus on similar principles with the main difference pertaining to the level and country of their implementation; local, national or international privacy regulations. Another interesting aspect is that much of their development is founded on existing standards, which are modified to comply with the context and regulations of the country in which the new standard is being implemented. If it is unnecessary to develop a new standard, the existing standard is implemented. For example, the PMM is based on GAPP and outlines the expectations of each level of the 73 criteria in GAPP (IAPP, 2011). HITRUST has established the Common Security Framework (CSF). This framework considers the requirements of existing standards and regulations, among others, HIPAA, NIST and the Control Objectives for Information and related Technology (COBIT) (http://www.hitrustalliance.net/about/). The EU data regulations, which are incorporated into the EU Data Protection Directive (known as

Directive 95/46 /EC), are based on the seven principles of the OECD relating to the privacy of personal records (Centre for Democracy and Technology, 2009).

A comparison conducted on nine of the aforementioned standards shows that most of the criteria correspond, while they may have different nomenclature (AICPA, 2005). The fact that the standards correspond and that most are developed from existing standards provides further evidence that the security and privacy standards and guidelines considered in this research adequately represent the field.

The three core properties that define information security are confidentiality, integrity and availability (ISO/IEC 27002, 2005; NIST Special Publication 800-53, 2009; ISO/IEC 27799, 2008). Additionally, for an application to be regarded as secure it needs to conceal information and resources; the data and resources have to be trustworthy; and the users must be able to utilise the required information or resource whenever they desire (Rozinov, 2004). Another criterion that needs to be considered is privacy. It is essential that the privacy rights of patients are strictly adhered to in health SN environments. Privacy is defined "as the area where information rights of different parties collide; it is fundamentally about the flow of personal information between parties that have different preferences in the manner in which that information should be utilized" (Brunk, 2005). This definition sufficiently describes the type of activities expected in health SN environments; the sharing of PHI; and the integration of services with third-party websites.

From the analysis of the security and privacy literature, it was determined that awareness, guidance, trust and feedback are equally important characteristics together with the core properties of information security. These have consequently been acknowledged and typified within the themes for the USec high-level heuristics. Accordingly, eight of the 16 USec high-level heuristics from table 4.3 and figure 4.8 originate from the security and privacy literature. These are visibility (characterises awareness and feedback), privacy, identity signal (characterises trust), availability, confidentiality, user assistance (characterises awareness and guidance), integrity and expressiveness/convey features (characterises guidance).

4.4.4 The High-level Heuristics and Checklist Items for Usable Security

As previously stated, the outcome from phase 1 of the process is 13 high-level heuristics for USec. Each heuristic has its own set of checklist items that assist experts to apply the heuristic in practice. These heuristics and their associated checklist items, which are the outcome of the first iteration, are presented in table 4.3 (Yeratziotis, Pottas & van Greunen, 2012).

Table 4.3: The USec HE after first iteration

1. Visibility – the system should keep users informed about their security status
1.1 If there are observable delays in the system's response time to a security-related action, is the user kept informed of the system's progress?
1.2 If pop-up windows are used to display security-related error messages, do they allow the user to see the field in error?
1.3 After the user completes a security action, does the feedback indicate that the next group of actions may be started?
1.4 Is there some form of feedback for every security-related action?
2. Revocability – the system should allow users to revoke any of their security actions
2.1 Do security options in menus make obvious whether de-selection is possible?
2.2 Can users easily reverse their security actions?
2.3 When prompts imply a necessary security action, are the words in the message consistent with that action?
2.4 Has the system been designed so that keys with similar names do not perform opposite (and potentially dangerous) security actions?
2.5 Can users cancel out of security operations in progress?
2.6 Is there an "undo" function at the level of a single security action or for a complete group of security actions?
3. Clarity – the system should inform users in advance about the consequences of any security actions
3.1 Are users prompt in confirming security actions that have drastic, destructive consequences?
3.2 Are the function keys that can cause the most serious consequences in hard-to-reach positions?
3.3 Does the system warn users if they are about to make a potentially serious security error?
3.4 Does the system prevent users from making security errors whenever possible?
4. Convey Features/Expressiveness – the system should guide users on security in a manner that still gives them freedom of expression
4.1 Are users' initiators of security actions rather than respondents?
4.2 Does the system correctly anticipate and prompt for the users' probable next security-related activity?
4.3 By looking, can the user tell the security state of the system, and the alternatives for security-related actions, if needed?
4.4 Is there a clear understanding of the system's security capabilities?
5. Learnability – the system should ensure that security actions are easy to learn and remember
5.1 Have security items been grouped into logical zones, and have headings been used to distinguish between the zones?
5.2 Does the system provide mapping: that is, are the relationships between security controls and security actions apparent to the user?
5.3 Are security operations easy to learn and use?
5.4 Are there security selection defaults?
5.5 Do GUI menus make obvious which security items are selected?
5.6 Does the system protect users from making severe errors?
5.7 Is security-related information presented in a standardised manner?
6. Aesthetics and Minimalist Design – the system should offer users relevant information relating to their security actions

6.1 Is only the security information essential to decision making displayed on the screen?
6.2 Are all security icons in a set visually and conceptually distinct?
6.3 Are security labels brief, familiar and descriptive?
6.4 Are security prompts expressed in the affirmative?
7. Errors – the system should provide users with detailed security error messages that they can understand and act upon
7.1 Are security-related prompts stated constructively, without overt criticism of the user?
7.2 Do security-related error messages inform the user of the error's severity?
7.3 Do security-related error messages suggest the cause of the problem?
7.4 Do security-related error messages indicate what action the user needs to take to correct the error?
7.5 Are the security-related error messages accurate in their descriptions?
8. Satisfaction – the system should ensure that users have a good experience when using security and that they are in control
8.1 Is each individual security setting a member of a family of security options?
8.2 Has colour been used specifically to draw attention and indicate status changes for security-related actions and information?
8.3 Do security-related prompts imply that the user is in control?
9. User Suitability – the system should provide options for users with diverse levels of skill and experience in security
9.1. If the system supports both novice and expert users, are multiple levels of security error message detail available?
9.2 Can users choose between iconic and text display of security information, where appropriate?
9.3 If the system supports both novice and expert users, are multiple levels of security detail available?
9.4 Can users easily change the level of security detail?
9.5 Can users easily change between novice and expert levels?
9.6 Can users customise security to meet their individual preferences?
10. User Language – the system should use plain language that users can understand with regard to security
10.1 Are security actions named consistently across all prompts in the design?
10.2 Are security objects named consistently across all prompts in the design?
10.3 Is security information accurate, complete and understandable?
10.4 Are security questions stated in clear and simple language, where used?
10.5 Is privacy jargon avoided?
10.6 Is security jargon avoided?
11. User Assistance – the system should make security help apparent for users
11.1 Is there a security help function visible (e.g. a key labelled "Security Help")?
11.2 Is the security information provided relevant?
11.3 Can users easily switch between security help and their work?
11.4 Do instructions follow the sequence of user security actions?
11.5 Does the system provide users with updated security educational opportunities, if they desire it?
12. Identity Signal – the system should have valid certificates and the information should be available on the browser of use
12.1 Does the system notify the users when they are interacting with non-trustworthy sources (non-trustworthy is a source that has no information about its identity)?
12.2 Is the information displayed in the identity signal derived from validated certificates?
12.3 Does the identity signal include human-readable information about the certificate subject?
12.4 Does the identity signal include the Issuer fields' organisation attribute to inform the user about the party responsible for that information?
12.5 Are there privacy indicators informing users about the privacy practices of the system?
13. Security and Privacy – the system needs to consider integrity, availability, confidentiality and privacy

13.1 Are protected areas completely inaccessible?

13.2 Can protected or confidential areas be accessed with certain passwords?

13.3 Is it clear that the users give consent regarding the use of their personal information?

13.4 Is it clearly stated for what purposes users' personal information is used?

13.5 Does the system grant access to a user based on valid authorisation?

13.6 Can the user update or delete inaccurate personal information?

13.7 In the case where the user must provide sensitive personal information, does the system state what measures are used to protect this data?

13.8 Does the system notify users on their access privileges?

13.9 Does the system initiate a session lock after a period of inactivity or upon user request?

13.10 Does the system enforce a limit of consecutive invalid access attempts by a user during a period of time?

13.11 Are notification messages relating to security and privacy displayed to the user before access to the system is granted?

13.12 Are there controls in place that will assist the user in making sharing/collaboration decisions?

13.13 Does the system ensure that publically accessible information does not contain non-public information?

13.14 Does the system install required software updates automatically and notify the user about this action?

13.15 Does the system employ automated tools that provide notification to the user upon discovering discrepancies during integrity verification?

13.16 Does the system notify the user about the procedure to be followed in the case of duplication or loss of personal information?

13.17 Does the system employ automated mechanisms to assist in the reporting of security incidents?

13.18 Does the system notify the user of any information system weaknesses or vulnerabilities associated with reported security incidents?

13.19 Does the system notify the user about the conduct of backups relating to their personal information?

13.20 Is there a backup policy that regulates how copies of information should be taken and tested regularly?

13.21 Does the system provide awareness and educate the user on how to complete tasks?

13.22 Does the system enforce minimum password complexity of defined requirements?

13.23 Does the system encrypt passwords in storage and in transmission?

13.24 Does the system enforce password minimum and maximum lifetime restrictions?

13.25 Does the system prohibit password reuse for a defined number of generations?

13.26 Does the system employ cryptographic mechanisms to prevent unauthorised disclosure of information during transmission?

13.27 Does the system require users to confirm statements indicating that they understand the conditions of access?

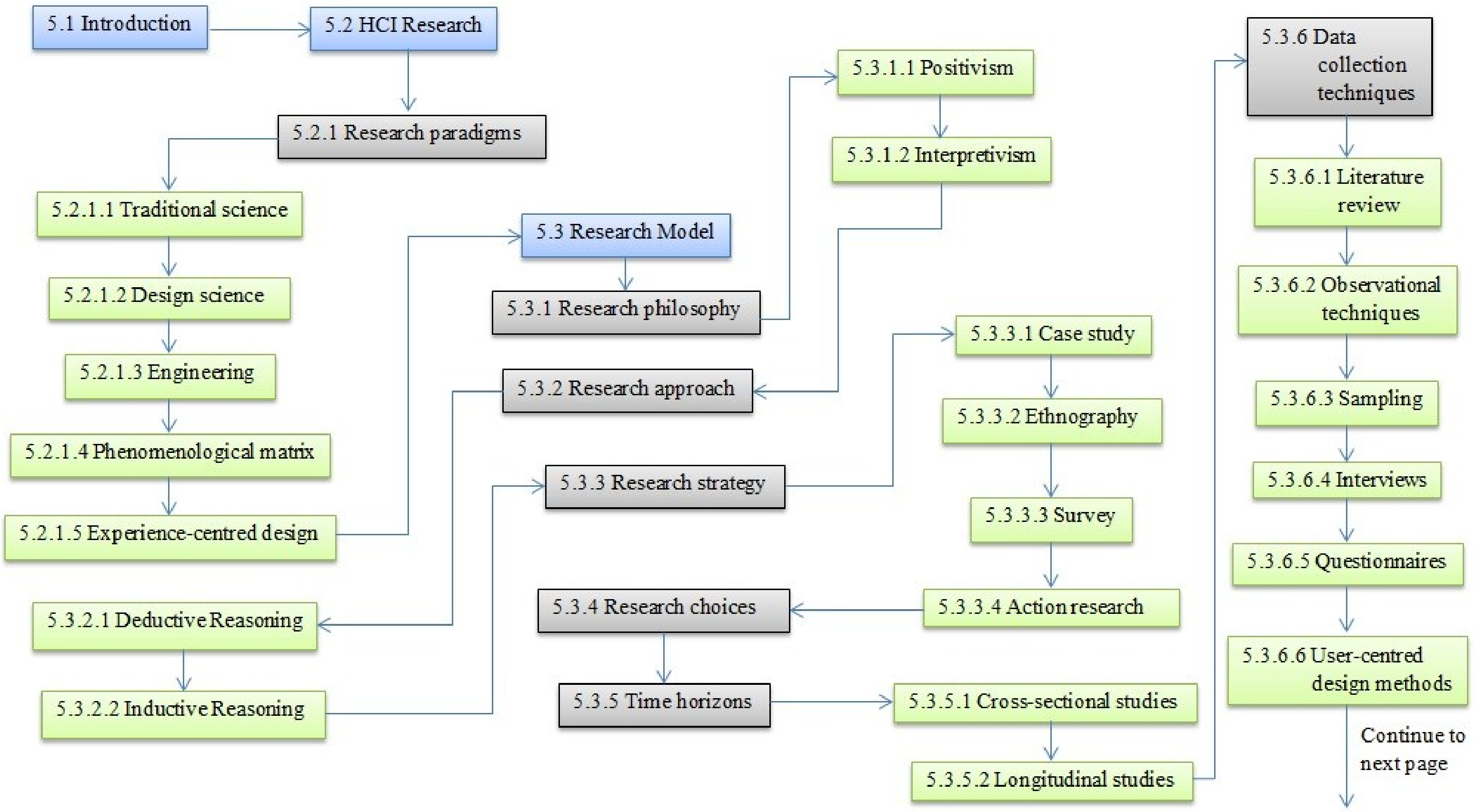
4.5 SUMMARY

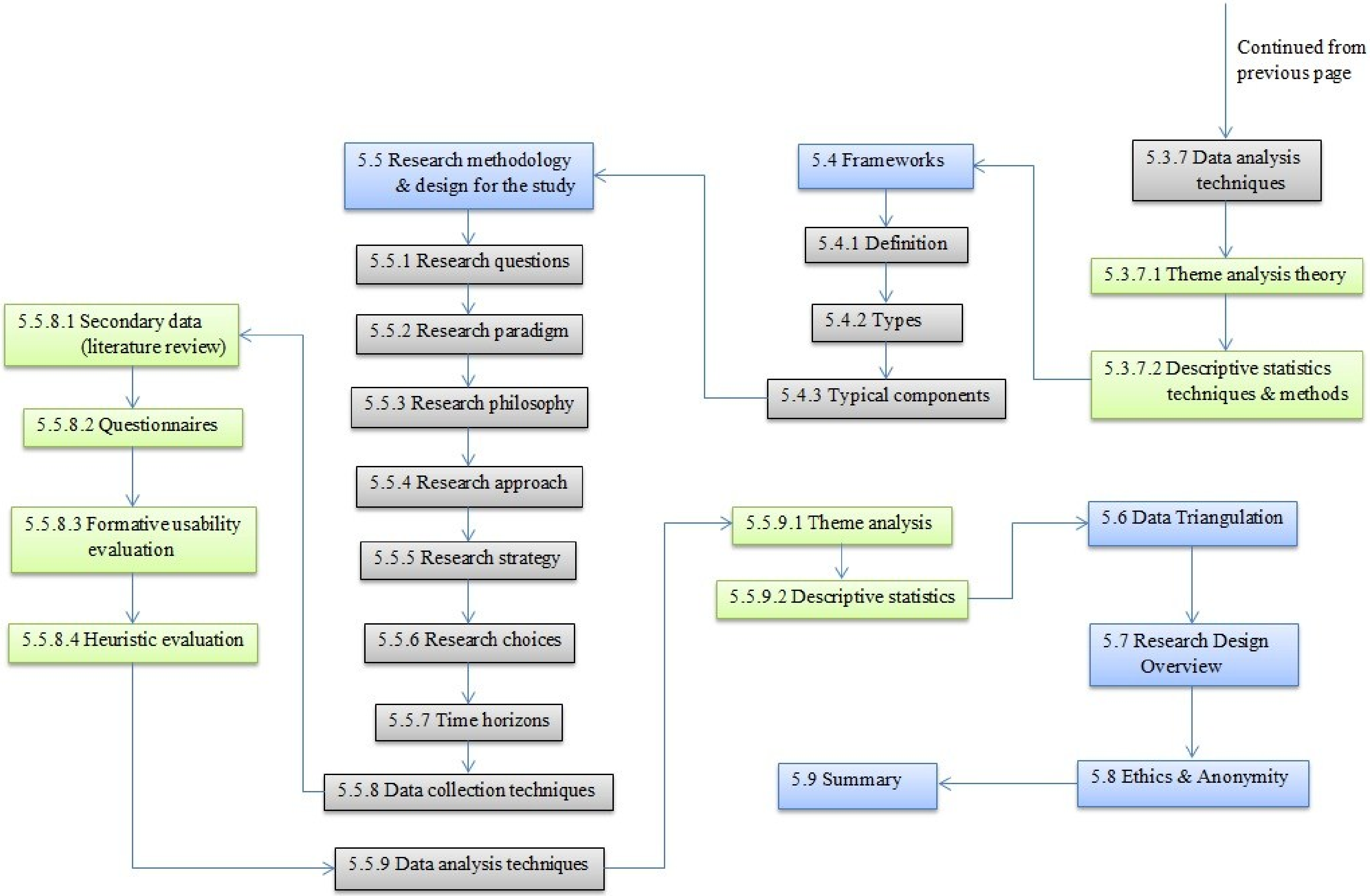
This chapter had two main intentions: firstly, to present the new process to develop heuristics for a SAD, and secondly, to present the USec heuristics and their checklist items. These were developed by following the proposed process. It should be noted that the heuristics presented in this chapter are the outcome of phase 1. The application and validation of the USec heuristics will be presented in chapters 6 and 7.

The chapter started with a discussion on a modified version of the HCD approach. In essence, the HCD activities were modified for the purpose of the new three-phase process. Yet, they still remained true to a human-centred approach to development. The modified activities are to understand and specify the context of use, specify the user and application domain requirements, produce high-level heuristics and checklist items and evaluate high-level heuristics with users and experts. The goal for this approach is to ensure that the heuristic set satisfies SAD requirements. A discussion on the three-phase process followed, with each phase and its associated tasks being introduced. The purpose of phase 1 is to design high-level heuristics and the required tasks for this phase include reviewing literature, naming high-level heuristics according to themes identified, tailoring existing heuristics to fit the SAD, grouping checklist items based on high-level heuristic names and reviewing the grouping of checklist items. The purpose of phase 2 is to validate the high-level heuristics that were developed in phase 1. The required tasks for this phase include identifying and selecting experts, applying the validation tool to validate the high-level heuristics, analysing review results and iterating and re-designing the high-level heuristics. The purpose of phase 3 is to apply the high-level heuristics in context. The required tasks for this phase include identifying and selecting appropriate applications/websites for the evaluation, developing scenarios and tasks for the evaluation, identifying and selecting users, applying high-level heuristics to evaluate the application/website, analysing user feedback of using the heuristics and iterating and re-designing the high-level heuristics. Once the three-phase process had been discussed, the 13 high-level heuristics for USec were presented. Each high-level heuristic consists of several checklist items. The high-level heuristics include Visibility, Revocability, Clarity, Expressiveness/Convey features, Learnability, Aesthetic and minimalist design, Errors, Satisfaction, User suitability, User language, User assistance, Identity signal and Security and privacy.

Based on the discussion in chapter 4, two sub-questions have been addressed. Firstly, a UIM has been adapted for USec in the form of a USec HE. Secondly, an approach that can be followed to create the USec HE has been developed in the form of a three-phase process to develop heuristics for SADs. The validity and applicability of both the method and the approach is tested in chapters 6 and 7, while the framework to evaluate USec is constituted in chapter 8. In chapter 5, the research design and methodology that were applied in this research are discussed.

LAYOUT OF CHAPTER 5




Continued from previous page
5.3.7 Data analysis techniques
5.3.7.1 Theme analysis theory
5.3.7.2 Descriptive statistics techniques & methods
5.4 Frameworks
5.4.1 Definition
5.4.2 Types
5.4.3 Typical components
5.5 Research methodology & design for the study
5.5.1 Research questions
5.5.2 Research paradigm
5.5.3 Research philosophy
5.5.4 Research approach
5.5.5 Research strategy
5.5.6 Research choices
5.5.7 Time horizons
5.5.8 Data collection techniques
5.5.8.1 Secondary data (literature review)
5.5.8.2 Questionnaires
5.5.8.3 Formative usability evaluation
5.5.8.4 Heuristic evaluation
5.5.9 Data analysis techniques
5.5.9.1 Theme analysis
5.5.9.2 Descriptive statistics
5.6 Data Triangulation
5.7 Research Design Overview
5.8 Ethics & Anonymity
5.9 Summary

CHAPTER 5: RESEARCH DESIGN AND METHODOLOGY

5.1 INTRODUCTION

Chapters 2 and 3 focused on the theoretical investigation and chapter 4 presented the new process and the USec heuristics and checklist items. The purpose of chapter 5 is to discuss the research design and methodology that will be applied in this study. This discussion is aligned to the research questions proposed in chapter 1. The way in which these are addressed will be elaborated on in this chapter. The chapter initially discusses theory regarding various research methodologies (sections 5.2, 5.3 and 5.4). Following the theoretical investigation is a discussion on the research design and methodology that have been applied to this study (sections 5.5, 5.6 and 5.7).

Section 5.2 will focus on the various research paradigms in HCI research and section 5.3 introduces a research model. In section 5.4 frameworks will be discussed, while the research model in section 5.3 is then adapted for this research and is discussed in detail in section 5.5. This section emphasises how the model is applied in the context of this study. Following this, section 5.6 contains a detailed discussion on the data triangulation process. An overview of the research design, based on the previously discussed sections, is presented in section 5.7. Ethical considerations are mentioned in section 5.8 and the summary is presented in section 5.9. The summary also includes a diagram (figure 5.16) illustrating the research methodological process, which clarifies the flow of the research design and methodology for this study.

5.2 HUMAN-COMPUTER INTERACTION RESEARCH

Research in the field of HCI is the focus of this section. This discussion extends to the types of paradigm in terms of which the research can be undertaken.

5.2.1 Research Paradigms

HCI is described as a multidisciplinary science and field (Carroll, 2003; De Villiers, 2005). It is defined as the following (Hewett et al., 1996, p. 5):

> *"HCI is the discipline concerned with the design, evaluation and implementation of interactive computing systems for human use and with the study of major phenomena surrounding them."*

In order to conduct research within the HCI field, one will first need to consider the paradigm in which the research process will be undertaken. Established and non-established paradigms will be introduced and briefly discussed in the subsequent sections. Established paradigms refer to those which have been commonly used in HCI research to date. Non-established are those that have been recently introduced in order to improve HCI research, although they lack the recognition of the established ones. The established paradigms applied, which cater for the multidisciplinary nature of HCI research include,

- traditional science
- design science
- engineering.

As mentioned previously, new paradigms are constantly being introduced for research in the HCI field. They attempt to accommodate the weaknesses that are inherent in the established paradigms. Nonetheless, it must be noted that they should not be regarded as replacements or disproval of the established paradigms. Instead, they are alternative ways in which to observe and think about, and consequently, conduct HCI research (Harrison, Tatar & Sengers, 2007). In fact, this is the purpose of all paradigms in any research area. Recently introduced or non-established paradigms for HCI research include

- phenomenological matrix
- experience-centred design.

The research paradigm that was chosen for this study is mentioned in section 5.5.2.

5.2.1.1 Traditional Science

When applying the paradigm of traditional science, the focus is on producing engineering-style theories and tools for designers (Newell & Card, 1986; Van Greunen, 2009). The resulting HCI knowledge will need to be expressed in engineering-style models of the user. Hence, empirical methods and quantitative data collection methods are used. Criticisms of these methods are their cost and lengthy time durations (Clark & Sasse, 1997; Van Greunen, 2009). The practice of design in the traditional science paradigm is based on scientific inquiry (Zimmerman, Forlizzi & Evenson, 2007).

5.2.1.2 Design Science

Zimmerman et al. (2007) refer to design science as design research. The impetus of this paradigm is to generate theories that address design challenges. This is accomplished by examining design in order to improve processes and by analysing design artefacts. A critical consideration for this paradigm is the relevance of the new knowledge to be generated. Theories are developed by exploring the interactions between humans and machines and by employing qualitative data collection methods. The fact that system design must consider issues beyond usability results in ideas that are less robust than those derived from more formal experimental paradigms (Clark & Sasse, 1997; Van Greunen, 2009).

5.2.1.3 Engineering

For an engineering paradigm, the foundation of research is built upon the accretion of knowledge and the formulation of engineering principles. Accordingly, user interface design and evaluations are conducted in accordance with research results. A blend of data collection methods, including quantitative and qualitative ones, is employed. Thus, the shortcomings of the traditional science and design science paradigms are compensated for. The main drawback of this paradigm is that the newly developed engineering principles are based on a notion that requires consent within the discipline. However, this consensus does not exist at present (Clark & Sasse, 1997).

Design as engineering is a substitute name for the paradigm. In this case, design is manipulated by means of a three-phase process. It begins with a problem statement or requirements. Then an abstract specification of the solution will pursue. Ultimately, an implemented solution results via a sequence of predefined steps. This paradigm ensures that the accumulated knowledge is independent of individual designers and that the research process may be replicated (Wright, Blythe & McCarthy, 2006).

5.2.1.4 Phenomenological Matrix

The focus of the phenomenological matrix rests solely on embodied interaction, even though it is also considered in other paradigms as well. When investigating human factors, issues such as readable font sizes or the fit of a mouse in the human hand are of interest, while cognitive-based work in HCI will examine physical constraints and improve interface design by measuring actions (e.g. the times to complete a task on the user interface). Embodiment in this paradigm is observed from a different perspective and is based on the phenomenological stance. Humans are considered embodied actors, and the manner in which they understand the world, themselves and interactions, is highly dependent on their location in the physical and social world. By focusing primarily on embodied interaction, what is fundamental to interaction substantially changes (Harrison et al., 2007).

Meaning and its creation, a key point in research, is derived on the fly via collaboration, by people in a particular context and situation. As a result, the interaction itself becomes a vital component in meaning construction. Owing to the paradigm's reliance on phenomenology, it is referred to as the phenomenological matrix. However, the name of the paradigm has caused distress in the research community. For this reason, the authors themselves have invited alternative names to be proposed by the research community, which they will subsequently consider (Harrison et al., 2007).

5.2.1.5 Experience-Centred Design

The key motivation for HCI research is the experience of the users. This has been repeatedly emphasised over the past few years and has raised considerable questions, the most prominent being: What is user experience and how should it be designed for? In order to answer this type of questions it is necessary to explore interdisciplinary literature. Furthermore, experience and technology should be placed at the heart of theory and design practice (Wright et al., 2006). Wright et al. (2006) characterise the paradigm in terms of three themes:

1. Experience must be considered as a holistic approach in which intellectual, sensual and emotional stands are equal partners in experience.
2. Oneself forms the centre of experience and promotes constant engagement and sense making. This results in a history of meanings and anticipated futures, which will assist in completing the experience using acts of sense making.
3. A relational approach based on the assembly of several centres of value, including self, object and setting, and multiple perspectives. This assembly permits an action, utterance or thing to be designed and produced. However, finalising it is not probable, since the experience of it is always concluded in dialogue with those other centres of value.

Design as radically interdisciplinary dialogue is the concept supporting the paradigm. The point being that HCI has developed vastly, and usability alone cannot solve challenges effectively on its own. Radical interdisciplinary research is necessary so that the arts and sciences can be merged. This is essential and will lead to solutions of "wicked problems". Wright et al. (2006) define *wicked problems* as those that are ill-formulated, potentially unbounded, open to alternative formulations with no obvious means of choice or stopping rule and are particular to a situation, setting or context. An example of a wicked problem is designing for experience. To summarise, HCI can be better understood by integrating radically interdisciplinary research and practice.

5.3 RESEARCH MODEL

The theory supporting the research paradigm is better understood by examining a research model, referred to as the research onion (Saunders, Lewis & Thornhill, 2007). This provides a suitable foundation for understanding the research process and may be customised accordingly to be applied in any research domain.

The model is comprised of six levels. The research process begins at the exterior of the onion ring. As it moves through the various levels, the interior core of the ring will be reached. This is the area where the data will be collected. The levels, stated from the exterior of the ring and moving towards the interior core of it include research philosophy, research approach, research strategy, choices, time horizons, and techniques and procedures. All levels will need to be considered, as they will direct the research process. The six levels and their related options are displayed in figure 5.1.

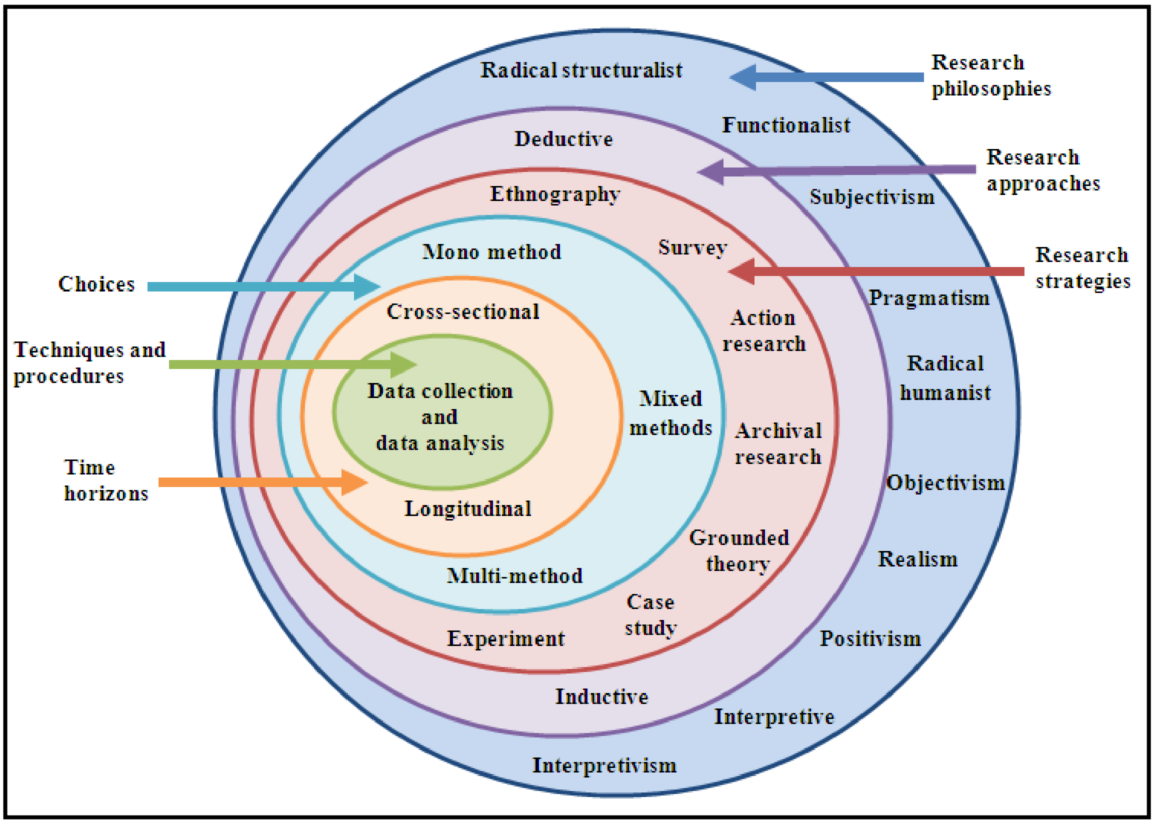


Figure 5.1: The research onion model (Saunders et al., 2007)

5.3.1 Research Philosophy

In figure 5.1, the research philosophy is represented in the first layer of the model, starting from the exterior of the ring. The research philosophy essentially describes the development of knowledge, as well as the nature of it (Saunders et al., 2007). In basic terms, it focuses on the path that one follows in an attempt to solve a specific problem. It contains important assumptions on how the researcher views the world. Therefore, the researcher takes a stance, which will direct the research strategies and methods to be employed.

Selecting a philosophy is influenced by the practical considerations of the research, as well as the researcher's view on the development of new knowledge and the process that it should follow. Hence, a researcher who is concerned with facts would use a different philosophy to one who is concerned with attitudes or feelings of people in a particular context and it is likely that their research strategies and methods would also differ. There are numerous philosophies that can be applied. Some are displayed in the research philosophies layer of the research onion in figure 5.1.

Two extreme philosophies will be examined in terms of this research: positivism and interpretivism. It is important to understand that one research philosophy is not superior to another. Rather, one should consider philosophies as better in doing different things. Deciding on which philosophy to deploy depends on the research questions and how they can be answered effectively. Although the onion portrays research as fitting into one of the philosophies, this is not always the case (Saunders et al., 2007). Instead, a mixture of philosophies is also commonly used. The research philosophy that was chosen for this study is mentioned in section 5.5.3.

5.3.1.1 Positivism

A positivist philosophy is aligned to the physical and natural sciences. Hence, it considers knowledge from a purely objective standpoint (Olivier, 2009). According to this philosophy, the researcher is independent and does not influence or get influenced by the research subject. In following positivist principles in the collection of credible data it is necessary to observe phenomena. The researcher will then need to use a research strategy to extract this data. Such a strategy is commonly based on analysing existing theory in order to develop hypotheses. Consequently, the hypotheses will be tested for their validity in an attempt to develop new theory (Saunders et al., 2007).

Complete independence from the research subject is also questioned, as it is regarded as near impossible task for researchers to be absolutely liberated from endorsing their own values within the research process. Positivism emphasises quantitative data collection methods that include statistical analysis. However, it is possible to adopt a positivist philosophy and combine qualitative data collection methods as well (Saunders et al., 2007).

5.3.1.2 Interpretivism

Unlike a positivist philosophy, where research needs to be objective, researchers may be required to take a more subjective approach. A philosophy that adheres to this is that of interpretivism, which states that it is necessary for the researcher to comprehend differences between humans in their roles as social actors. This is not just based on understanding objects (e.g. computer), but rather on how humans would interrelate with such an object.

Interpretivism originates from two scholarly traditions, phenomenology and symbolic interactionism. Phenomenology focuses on understanding how humans make sense of the world around them, while in symbolic interactionism the researcher has to interpret the actions of the subjects, as they interact with each other and other objects. This will guide the researcher to adjust personal meanings and actions (Babbie, 2005). To successfully employ an intepretivist philosophy, it is critical that the researcher adopt a considerate attitude during the entire process. The challenge is to enter the world of the subjects and understand their perspectives in terms of actions and meanings (Saunders et al., 2007).

5.3.2 Research Approach

In figure 5.1, the research approach is represented in the second layer of the model, starting from the exterior of the ring. The research onion provides two alternatives with regard to the research approach – inductive and deductive reasoning. The research approach to be selected depends on how theory is used in the study. It also addresses important aspects relating to the design of the research project. In essence, in deductive reasoning, theory and hypotheses are developed. Subsequently, research strategies will be selected to test the hypotheses. In contrast, in inductive reasoning, data are collected and theory is developed based on the analysis of the data (Saunders et al., 2007). More details on the two approaches are discussed in the following sections.

Figure 5.2 compares the logic and the steps that are followed in the two approaches. Of significance is the theoretical component. Understanding how this is applied within each approach will assist in determining which approach to apply. The main difference is that in deductive reasoning one will confirm theory, while in inductive reasoning one will develop theory from observation.

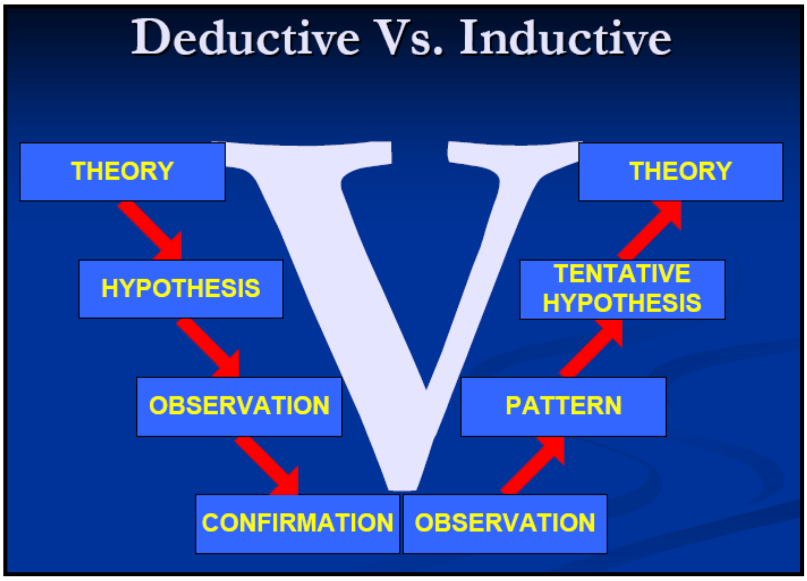


Figure 5.2: Logic supporting the two research approaches (Trochim & Donelly, 2006)

The fact that there are clear distinctions between the characteristics of each approach can be misleading. Thus, it is possible to combine the approaches within the same research. In point of fact, it is considered advantageous to do so. The research approach that was chosen for this study is mentioned in section 5.5.4.

5.3.2.1 Deductive Reasoning

Deductive reasoning relates more to the scientific approach. Theory will be subjected to rigorous testing, in an attempt to explain or confirm it. This is characterised by the following: explaining a relationship between variables, identifying a form of relationship between the variables, and testing hypotheses to confirm if the relationship assumption is correct. Quantitative data are used to test the hypotheses.

Also referred to as the “top-down” approach, this approach begins with a specific theory about a topic of interest. Once this theory has been investigated, it will be narrowed down to particular testable hypotheses. As a result, further observations are determined. These observations will then be employed to address the hypotheses (research questions or goals) for confirmation of the original theories (Saunders et al., 2000). The deduceive reasoning process is displayed in figure 5.2.

5.3.2.2 Inductive Reasoning

Inductive reasoning is in contrast to deductive reasoning and follows a "bottom-up" approach. The process begins with specifics and proceeds towards generalisations (Merriam, 2001). The researcher begins with specific observations and measures from which patterns and regularities are detected, which help formulate tentative hypotheses in the form of research questions or goals. These are explored in depth in order to develop some general conclusions or theories (Saunders et al., 2007).

In the inductive approach, theory follows the data. However, the opposite happens in the deductive approach. Representative of the inductive approach is research that considers context. Thus, the particular context in which an event occurs is of foremost importance (Saunders et al., 2007).

Table 5.1 summarises deductive and inductive reasoning and focuses on the major differences between the two approaches, in terms of what they tend to emphasise during the research process.

Table 5.1: Differences between the deductive and inductive approaches (Saunders et al., 2007)

Deductive emphasises	Induction emphasises
Scientific principles	Gaining an understanding of the meanings humans attach to events
Moving from theory to data	
The need to explain causal relationships between variables	A close understanding of the research context
The collection of quantitative data	The collection of qualitative data
The application of controls to ensure validity of data	
The operationalisation of concepts to ensure clarity of definition	
A highly structured approach	A more flexible structure to permit changes of research emphasis as the research progresses
Researcher independence of what is being researched	A realisation that the researcher is part of the research process
The necessity to select samples of sufficient size in order to generalise conclusions	Less concern with the need to generalise

5.3.3 Research Strategy

In figure 5.1, the research strategy is represented in the third layer of the model, starting from the exterior of the ring. There is a wealth of research strategies to select from and such strategies can be employed for exploratory, descriptive and explanatory research. Although some of them belong to a deductive approach and others to an inductive one, as previously mentioned, it is misleading to allocate strategies to a single approach. In addition, there is no strategy that is superior to another. The best strategy to use is the one that will enable the researcher to answer the research questions addressed, as well as assist in achieving the research objectives. Hence, the factors that will influence the selection of the strategy/strategies include research questions, research objectives, existing literature, available time, and the researcher's philosophical beliefs (Saunders et al., 2007).

A common way in which research strategies are categorised is as quantitative or qualitative research methods. The purpose of the quantitative methods is to measure (quantify) the relationship between two or more things and then attempt to present this in a statistical or numerical format. On the other hand, with qualitative data the intention is to identify the quality of the relationship that exists between two or more things. This relates directly to the researcher's intentions to make sense of the interpretations, as well as to assign meaning to the way people do and understand things (Myers, 1997). Many researchers share the view that quantitative and qualitative methods should be used together in order to complement one another, rather than to rival each other (Trauth & Jessup, 2000). Qualitative and quantitative research methods are displayed in figure 5.3, which situates them on a positivism vs. interpretivism philosophy continuum.

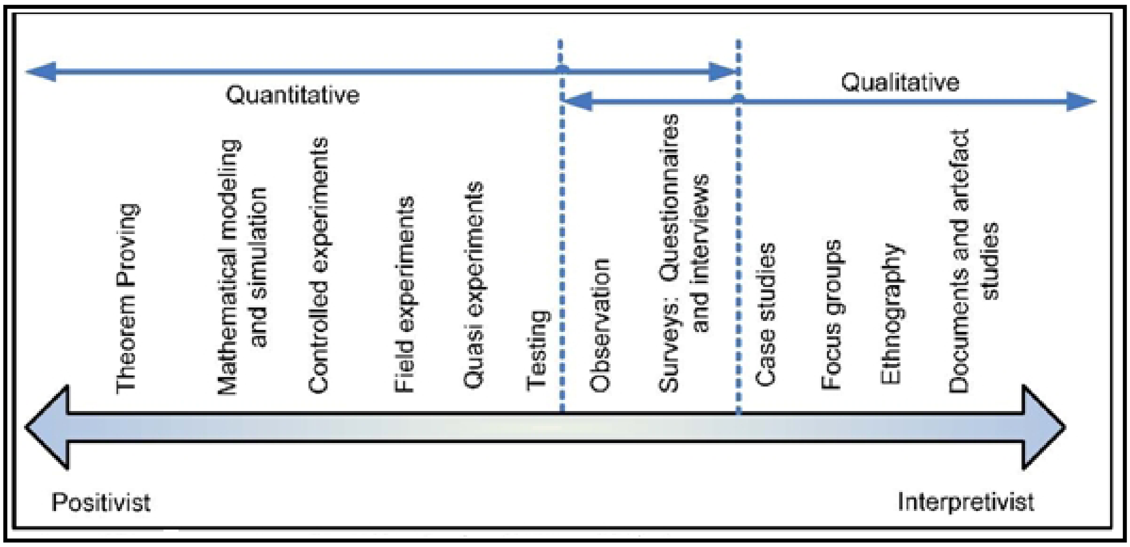


Figure 5.3: Research strategies that are representative of the positivist and interpretivist philosophies (De Villiers, 2005, p. 112)

In this section, four research strategies will be discussed in more detail. These are case study, ethnography, survey, and action research. The reason why these are further elaborated on is because they are all suitable candidates, in terms of a research strategy, for addressing the primary and sub research questions, which were set out in chapter 1. In fact, more than one strategy can be combined. Nonetheless, other prominent strategies, which are used as part of positivist and interpretivist philosophies, are also defined in table 5.2. Furthermore, these strategies are classified as quantitative or qualitative realisations in the table. In some cases, the strategy may be applied in both realisations, as is displayed in figure 5.3. The research strategy that was chosen for this study is mentioned in section 5.5.5.

Table 5.2: Qualitative and quantitative research methods (Saunders et al., 2007; Olivier, 2009)

Method	Description	Realisation
Experiment	Used to test or prove a theory.	Quantitative
Focus group	Similar to a brainstorming session, where a small group of people interact in order to stimulate thinking and creativity.	Qualitative
Archival research	Uses administrative records and documents as the main source of data.	Qualitative
Action research	Iterative process to determine the current situation of a focus area in order to make an intervention.	Qualitative
Ethnography and participant observation	Participants are studied within their field of work over a specified period of time.	Both
Grounded theory	Observation within the field of interest leads to the emergence of theory (contrast to the experiment).	Qualitative
Case study	Used to explore entity/entities restricted by time and activity. Can employ multiple data collection methods during the process.	Qualitative
Survey	Used to collect a large quantity of data from considerable populations in a highly economical way.	Both
Mathematical proofs	One of the single ways to demonstrate the absolute truth of a statement. Basically used to prove assertions mathematically.	Quantitative

5.3.3.1 Case Study

A case study is a very useful technique for extracting a lot of information about a specific member or subject. This method offers the researcher the possibility to study the subject in much more detail than most other research methods (Olivier, 2009). Robson (2002) provides the following definition: “A case study involves an empirical investigation of a particular contemporary phenomenon within its real life context using multiple sources of evidence.”

A significant aspect of a case study, which is constantly highlighted, is the importance of context (Yin, 2008; Saunders et al., 2007). This relates to the fact that the boundaries of the examined phenomenon and the context within which it is examined are not clearly apparent, unlike the experiment strategy, for example, in which the research process is undertaken in an extremely controlled context.

Four types of case study strategies can be determined according to two distinct dimensions: single vs. multiple case, and holistic vs. embedded case (Yin, 2008). A single case study focuses on a unique case. In contrast, a multiple case study strategy would entail examining more than one case. A multiple case study strategy is considered to be the preferable approach, as findings may be generalised (Yin, 2008). For the second dimension, a holistic case is employed when the research focuses on a single entity as a whole (e.g. the whole organisation). In the embedded case, the researcher explores different aspects within a single entity (e.g. sub-units or departments of the organisation).

In terms of IT research, case studies can offer a complete representation of users' experiences when interacting with a certain application, as they help in evaluating the effectiveness of the application by identifying its strengths and weaknesses. Hence, its successes and failures will provide a wide range of constructive information, which can then be analysed. Based on the analysis, patterns in the data will emerge. Once all the data have been collected, further analysis will be conducted. Once the appropriate changes identified by the case study have been recommended and implemented, the overall system should be improved (Patton, 1990).

5.3.3.2 Ethnography

Ethnography is derived from the anthropological practice of immersion in other cultures with the intent to understand and express social reality about the tested culture (Bhattacherjee, 2011; Millen, 2000). In ethnography, the research participants are treated as a "foreign tribe", while the researcher acts as an anthropologist who is studying the culture of this "tribe" (Millen, 2000). The research participants are studied in their natural settings or fields (Olivier, 2009), despite the fact this can result in a biased understanding of the activities conducted from the informants' perspective (Millen, 2000).

In order to conduct ethnography, it is important that the researcher is part of the community that is being explored. Hence, the researcher will only understand how the community operates by experiencing that culture as a member (Olivier, 2009). Owing to the researcher's immersion in the culture, their specific role and involvement in terms of the research process must be clarified during data analysis (Bhattacherjee, 2011).

The primary method of data collection is participant observation. Accordingly, analysing the data requires researchers to "make-sense" of it. Researchers support their "sense-making" approach with extensive field notes and by narrating their experiences in extensive detail. This allows readers to experience the culture via the researchers. The dual roles of researchers in ethnography are to generate theory by relying on their unique knowledge and engagement and to convince the scientific community of the nature of the studied phenomenon (Bhattacherjee, 2011).

A classic example of ethnographic research is Jane Goodall's study of primate behaviour. In order to understand them she had to live with chimpanzees in their natural habitat. Another example is Myra Bluebond-Langer's study of the experiences of children with life-threatening illnesses and their families. In this study the researcher followed 80 children for a period of over two years (Bhattacherjee, 2011).

5.3.3.3 Survey

A survey is a classic well-known research strategy commonly used as a form of observation in the social sciences. Essentially, the researcher will select a sample group of participants and administer a standardised survey to each one of them (Babbie, 2005).

The survey will be used to count "things" within some group. Such a group is also commonly referred to as the population group. In terms of this method, members of one population group, which share some common characteristics, will be compared to another population group that does not have similar characteristics (Olivier, 2009). This is a useful strategy to apply when determining correlations between characteristics. However, it does not show causation of a phenomenon, which an experiment does, for example.

Surveys have to be well planned and done accurately. If not, the results can be skewed, which will lead to invalid conclusions. This is a drawback of a survey strategy and one that will need to be considered. There are various data collection techniques that belong to the survey strategy, for example questionnaires, structured observation and structured interviews (Saunders et al., 2007).

5.3.3.4 Action Research

A common characteristic of action research is that it concentrates on contributing a solution to a situation to those who are experiencing it directly. Accordingly, the solution is based on change and includes the involvement of both practitioners and researchers. Therefore, the researcher forms part of the situation in which the change process is occurring. It is also based on an iterative process, which is comprised of the following steps: diagnosing, planning, taking action, and evaluating. The iterative process is displayed in figure 5.4.

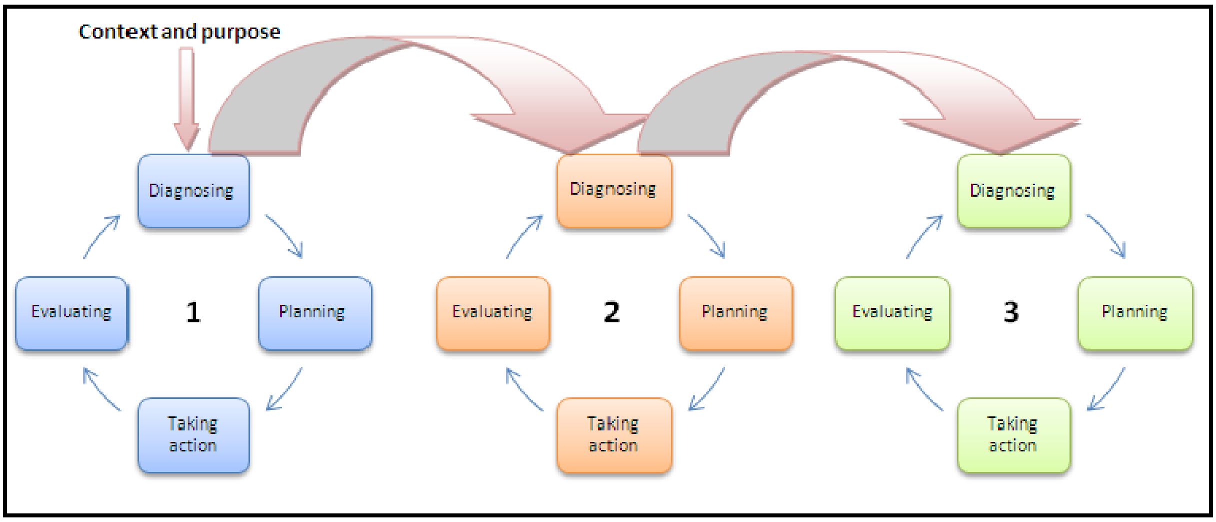


Figure 5.4: The action research spiral (Saunders et al., 2007)

The strength of this strategy is its focus on change, the allocation of appropriate time for the iterative steps, and the involvement of subjects throughout the research process. There are many definitions for action research; Babbie (2005) provides the following one: "Action research is an approach to social research in which the people being studied are given control over the purpose and procedures of the research; intended as a counter to the implicit view that researchers are superior to those they study."

Action research is an interactive method of inquiry that is well suited for investigating complex social phenomena. Consequently, these phenomena are better understood by introducing changes or actions and observing their effects. It is also a useful method for studying a social problem, as it provides learning and insights of how an action influences a phenomenon. An example of action research is to introduce organisational change programmes (e.g. new technology, processes or procedures) with the goal of improving profitability or performance. Theory must guide the researcher's actions by explaining why and how the actions may bring forth the desired social change (Bhattacherjee, 2011).

5.3.4 Research Choices

As previously mentioned, there are both qualitative and quantitative research methods. Quantitative methods imply numeric data, while qualitative methods imply non-numeric data. The manner in which the researcher decides to combine the two techniques comprises the research choice. In figure 5.1, the research choice is represented in the fourth layer of the model, starting from the exterior of the ring. The division of the research choices is displayed in figure 5.5.

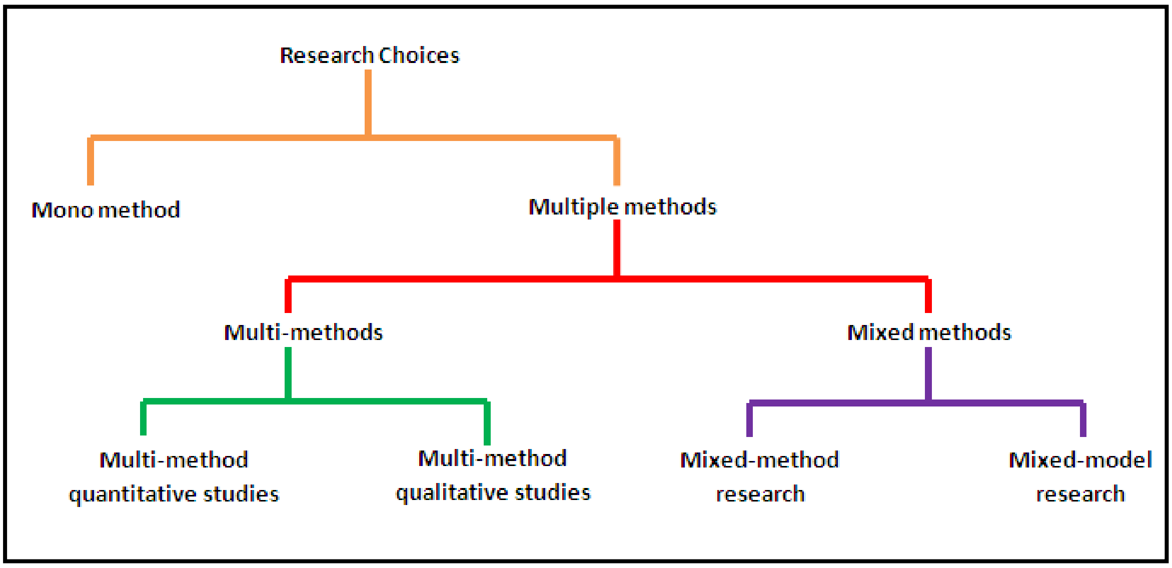


Figure 5.5: The research choices (Saunders et al., 2007)

In the case of a single data collection technique and its analogous analysis procedures, a mono method is used. Accordingly, one will combine a quantitative data collection technique with quantitative data analysis procedures or a qualitative data collection technique with qualitative data analysis procedures. If more than one data collection technique and analysis procedures are applied, then the multiple methods choice is used. This infers the use of numerous techniques in a single research study. The research choice that was chosen for this study is mentioned in section 5.5.6. In terms of the multiple methods choice, there are four different possibilities that a researcher could explore. They include the following (Saunders et al., 2007):

1. *Multi-method quantitative studies*. Implies the use of multiple quantitative data collection techniques and the use of quantitative procedures for the analysis.
2. *Multi-method qualitative studies.* Implies the use of multiple qualitative data collection techniques and the use of qualitative procedures for the analysis.
3. *Mixed-method research*. Implies the use of both quantitative and qualitative data collection techniques for the analysis. It is important to note that they are used either in parallel or in sequential order, but not in combination. Thus, quantitative data are analysed quantitatively and qualitative data qualitatively (Creswell, 2009).

4. *Mixed-model research*. Implies the use of both quantitative and qualitative data collection techniques for the analysis. In this case, however, they are combined. Therefore, it is possible to "qualitise" quantitative data and to "quantitise" qualitative data.

5.3.5 Time Horizons

Following the decision of which research choice to use are the time horizons. In figure 5.1, the time horizon is represented in the fifth layer of the model, starting from the exterior of the ring. There are two options relating to the time horizons layer. Either a cross-sectional or a longitudinal study may be conducted. Based largely on the research questions, one of the two will be utilised (Saunders et al., 2007). The time horizon that was chosen for this study is mentioned in section 5.5.7.

5.3.5.1 Cross-sectional Studies

This type of study tends to focus on the examination of a phenomenon (or phenomena) during a particular time frame. Accordingly, researchers attempt to describe their incidence and the relationships that occur within them. These are commonly related to academic work where time constraints exist. Nonetheless, an academic course may provide sufficient time for a longitudinal study as well (Babbie, 2005; Saunders et al., 2007).

Cross-sectional studies often use a survey strategy, as they are regarded as exploratory and descriptive studies; however, qualitative methods can also be employed. Because observations and generalisations are made during a single time only, bias becomes a concern. To counter this, revisiting the phenomenon at a different time and building on previous results is advised (Babbie, 2005).

5.3.5.2 Longitudinal Studies

This type of study tends to focus on the examination of a phenomenon (or phenomena) over an extended time frame. Its strength lies in the fact that it has the ability to examine change and development over time. This also assists the researcher in exercising more control over the variables being studied during the research process.

In longitudinal studies, observations and analyses can be made over the course of events that are being examined or at one time only. Babbie (2005) identifies three special types of longitudinal studies. They include:

- *Trend study*. This is used to monitor a specific characteristic of a population over a period of time.
- *Cohort study*. This is used to study a specific subpopulation (or cohort) over a period of time. The data may be gathered from different members during each set of observations.
- *Panel study*. This is used to collect data from the same set of participants (specific sample) at different points in time.

5.3.6 Data Collection Techniques

Data collection techniques assist with collecting and analysing the data. These are represented as techniques and procedures in the research onion model and are used as part of the overall research strategy or strategies that are implemented. In figure 5.1, these are represented in the centre of the model. The main data collection techniques include literature review, observational techniques, sampling, questionnaires, interviews, and usability methods. Each one of these techniques can contain various options within them, as will be shown. The data collection techniques that were chosen for this study are mentioned in section 5.5.8.

5.3.6.1 Literature Review

Literature has a fundamental role to play in any study, as one has to examine the relevant existing information on the research topic. Thus a literature review provides a method for understanding and obtaining an insight into previous research on the topic (Olivier, 2009). The literature review technique can be divided into three categories (Saunders et al., 2007):

- *Primary literature*. Also referred to as the grey literature. This is the first point from which a piece of work will originate. It includes published sources, like reports, and central and local government publications, such as white papers and planning documents. Unpublished manuscript sources, such as letters, memos, committee minutes also apply, as they can be analysed as data as well.
- *Secondary literature*. There is a wealth of secondary data available that keeps on expanding rapidly, largely due to the Internet. Such resources include books, journals, publications of primary literature, newspapers, and certain government publications. Secondary literature is easier to locate than primary literature.
- *Tertiary literature*. Also referred to as search tools. These are designed to assist one in locating primary and secondary literature or to introduce topics. The more popular

tools include indexes, abstracts, catalogues, encyclopaedias, dictionaries, bibliographies, and citation indexes.

5.3.6.2 Observational Techniques

When research questions and objectives are concerned with what people do, the observational technique can be employed. This will help the researcher discover this information by watching (observing) the research participants. In essence, observation includes systematic observation, recording, description, analysis and interpretation of human behaviour. Saunders et al. (2007) describe two types of observation technique:

- *Participant/user observation*. This is a qualitative technique that focuses on discovering the meanings that people attach to their actions. It originates from the field of social anthropology and is an unstructured and unsystematic observation approach. In terms of this technique, the observer can adopt any of four different roles: complete participant, complete observer, observer as participant, and participant as observer.
- *Structured/fieldwork observation*. This is a quantitative technique that focuses more on the frequency of people's actions. Hence, it is concerned with quantifying behaviour and is based on a predetermined structured and systematic approach. This technique implies that the observer adopts a more detached stance.

5.3.6.3 Sampling

Sampling is a technique that may be required for any research study, irrespective of the research questions and objectives at hand. In certain cases it may be acceptable to collect and analyse data from every possible group member. However, there are cases where this is not possible. Factors that contribute to this include the restriction of time, money and access. In these particular cases, the sampling technique provides a useful solution, as it enables the researcher to reduce the amount of data that will need to be collected by focusing on a subgroup rather than all group members. This assists in generalising results according to the sample (also referred to as the population) that is selected. There are two types of sampling technique (Oates, 2006):

- *Probability/representative sampling*. In terms of this type, the selected sample is based on the researcher's belief that there is a high probability the sample is representative of the overall population being examined. Therefore, it is possible to answer research questions and objectives that require the statistical estimation of characteristics relating to the sample population.

- *Non-probability/judgmental sampling*. In terms of this type, the researcher is unsure whether the sample population is representative of the overall population. This is due to the fact that members have unique characteristics that are not shared with other members of the sample group. At best, this method provides for weak generalisations to the wider population. Consequently, it is not used to make statistical inferences about the characteristics of the population.

5.3.6.4 Interviews

A simple definition of an interview is provided by Kahn and Cannell (1957), which they describe as a purposeful discussion between two or more people. Interviews are regarded as a useful technique to collect valid and reliable data relating to specific research objectives and questions. In the case where there are no research objectives and questions defined as yet, they can also assist in establishing them. Figure 5.6 displays the categorisation of interviews.

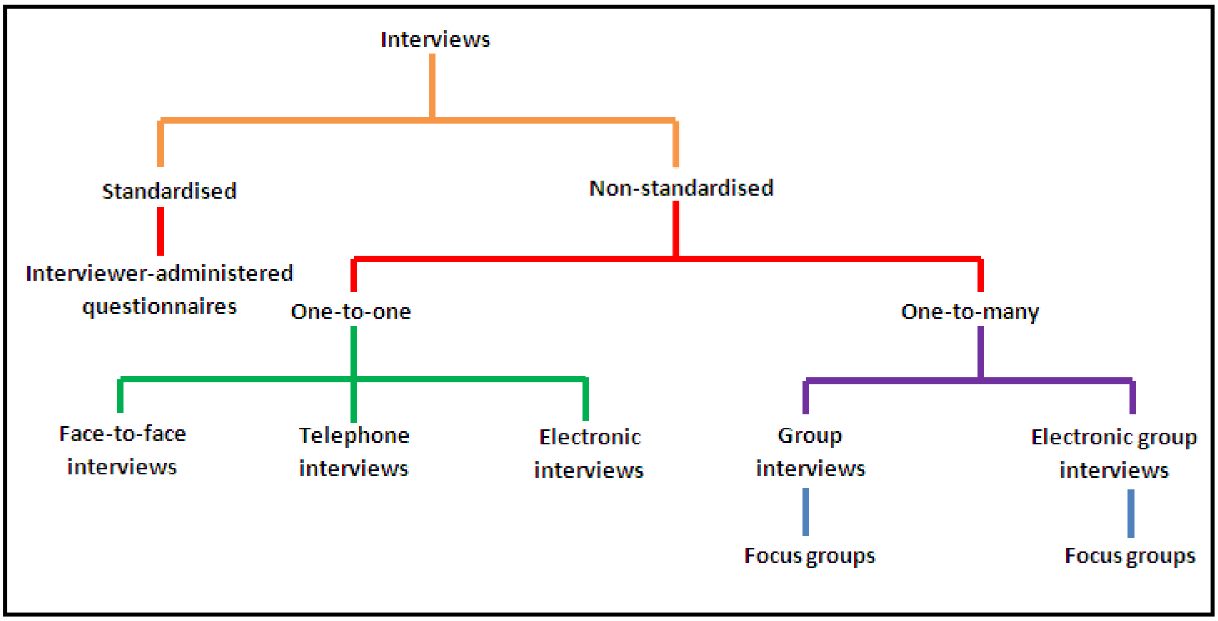


Figure 5.6: The categorisation of interviews (Saunders et al., 2007)

There are different types of interview, which are defined by different typologies. A common typology that is used is the level of formality and structure that is associated with the interview. On the basis of the formality typology, there exist three categories of interviews (Saunders et al., 2007):

- *Structured interview*. Questionnaires are used for the interviews in this category, and they are commonly referred to as interviewer-administered questionnaires. They include predetermined and standardised questions, which focus on collecting quantitative data. Questions are answered according to a predefined structure.

- *Semi-structured interview*. The questions in this category are not standardised and focus on collecting qualitative data. Rather, the interviewer may select what to discuss from a list of themes and questions, which tends to vary from interview to interview. The order of questions is not structured and can be varied depending on the discussion.
- *Unstructured or in-depth interview*. As with a semi-structured interview, this category is not standardised and focuses on the collection of qualitative data. Such interviews are regarded as informal interviews and are used to explore a general area of interest in depth. A predetermined list of questions does not exist, yet the interviewer will need to have a clear idea of the aspects that will be explored.

5.3.6.5 Questionnaires

Babbie (2005) defines a questionnaire as a document that contains questions and other types of items to extract information appropriate for analysis. Questionnaire are used mainly in a survey strategy but can also be used in case studies, experiments, field research and other modes of observation (Babbie, 2005; Saunders et al., 2007). DeVaus (2002) states that a questionnaire includes all techniques of data collection that focus on a set of questions, which are presented in a prearranged order. Accordingly, each person (participant) will need to respond to the same set of questions. In terms of the interview technique discussed previously, a questionnaire could include a structured interview, a telephone questionnaire, and questionnaires that are answered without the presence of an interviewer.

To develop a successful questionnaire, one will need to first consider the length of it. If the questionnaire is too long, the response rate could be low. The fact that they can be time consuming to develop is also a critical consideration. This is because pilot studies will need to be conducted first in order to eliminate potential misunderstandings in terms of the items of the questionnaire (Bernardo, 2005). Nonetheless, there are also key advantages with implementing questionnaires. The Internet provides a gateway to distribute them, which can result in a large response for a minimum cost. They also tend to be very versatile because they may be used at any stage of the design process. Moreover, the fact that they may be used anonymously can prevent researcher biases. Finally, they may be used repeatedly and for collecting subjective information regarding user preferences (Bernardo, 2005).

There are various questionnaire designs, which are based on the manner in which they are administered or the level of contact that interviewer has with the respondents. Therefore, two main categories can be identified, the subdivisions of which are displayed in figure 5.7. The two categories of questionnaire include the following (Saunders et al., 2007):

- *Self-administered questionnaire*. This type is usually completed by the respondents. They are administered by various means, as is displayed in figure 5.7.
- *Interviewer-administered questionnaire*. This type is usually recorded by the interviewer on the basis of responses from the respondents. It is administered in two ways, as is displayed in figure 5.7.

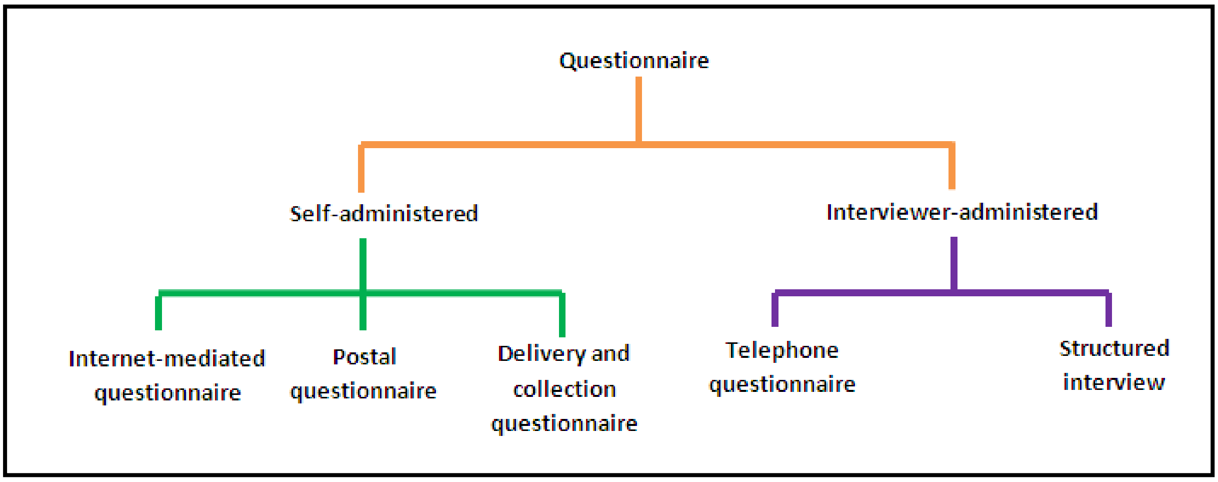


Figure 5.7: The categorisation of questionnaires (Saunders et al., 2007)

5.3.6.6 User-Centred Design Methods

User-centred design methods or UIMs are techniques used for the evaluation and development of products and services (e.g. software, websites, mobile phones). They require the continuous involvement of users in the design and evaluation phases and emphasise the application of usability practices to meet the needs and abilities of the users (BoK-a, 2005). User needs will be combined with business requirements in order to achieve effective UX (BoK-b, 2005). UIMs are discussed in detail in chapter 2.

5.3.7 Data Analysis Techniques

Data analysis techniques are used to process data and transform it into information from which conclusions can then be made. There are a variety of techniques and approaches for data analysis available, which can offer better analysis, depending on the research domain (e.g. business, science, and social science). Data analysis has multiple facets and approaches, encompassing diverse techniques under a variety of names, in different domains. Two techniques applied in HCI research are theme analysis and descriptive statistics.

5.3.7.1 Theme Analysis Theory

In an attempt to analyse the collected data in a qualitative research study, it is necessary to code the data. Creswell (2004) states that the purpose of the coding process is "to extract meaning from the text data, divide it into text or image segments, label these segments with codes for overlap and redundancy, and collapse these codes into broad themes". The codes are the labels that will be used to describe a segment of the text (e.g. setting and context, participant, activity etc.). Furthermore, Creswell (2004) proposes several steps to code the data. The step that is of a particular interest to this research is the step involved in developing themes (or categories).

Three common alternatives in selecting the format of analysis to follow include thematic analysis, content analysis and discourse analysis. Thematic analysis is the most approach suitable for this research. In this case, data are analysed according to theme and follow qualitative and inductive approaches as well. Data collection and analysis occur concurrently and research literature forms part of the analysis process. Thematic analysis is also connected to comparative analysis. In comparative analysis, data from various users is compared and contrasted until the researcher is satisfied with the results. On the other hand, content analysis tends to follow a quantitative approach; while discourse analysis resides somewhere between the quantitative and qualitative approaches and focuses on analysing patterns of speech. Therefore, the analysis is intuitive and reflective but may also involve some form of counting or measurement. Important considerations for all forms of analysis include the following (Creswell, 2004):

- Consider the data from the moment the information is being collected.
- Consider the value of the data (what or who the sources are).
- As the research progresses, the data must be interpreted in a meaningful manner and in an understandable format.
- Consider the mechanical processes that need to be undertaken to analyse the data

5.3.7.2 Descriptive Statistics Techniques and Methods

Descriptive statistics assist the researcher to understand more about the research data by assisting him or her to organise and summarise it (McHugh & Villarruel, 2003). This can be accomplished by means of tables and graphical displays (Trochim, 2006a).

Descriptive statistics are commonly used in two ways: firstly, in the form of an end point in the data analysis, which occurs in purely descriptive studies and, secondly, in the form of a starting point in the data analysis, which occurs before testing certain hypotheses with inferential statistics in the experimental research (McHugh & Villarruel, 2003). The difference between the two is that with inferential statistics one's efforts attempt to reach conclusions that extend beyond the direct data alone, namely to the population from which the sample was drawn; while in descriptive statistics one is simply describing what the data portray. Both of these techniques are recognised as quantitative methods for analysing data (Trochim, 2006a). Methods that can be used in descriptive statistics include graphs, frequency tables, means, standard deviations, factor analysis and reliabilities.

5.4 FRAMEWORKS

The primary objective of this study is to develop a framework for evaluating USec in online social networking environments. As a result, we need to understand what a framework is and how it can be developed. The purpose of this section is to define frameworks in general and describe typical components.

5.4.1 Definition

The term *theoretical* (or conceptual) *framework* includes a system of concepts, assumptions, expectations, beliefs and theories, which support and inform a particular research. It represents an integral part of design. A definition provided by Miles and Huberman (1994), states that it is "a visual or written product that explains, either graphically or in a narrative form, the main aspects to be studied. It includes key factors, concepts, variables and the presumed relationships among them".

Lethbridge and Laganiere (2005) mention that a framework needs to guide the research and also help identify which variables must be measured and what relationships to be aware of and thus their definition is that a framework is "an underlying set of ideas that includes, a set of ideas, principles, agreements, or rules that provides the basis or outline for something intended to be more fully developed at a later stage".

When conducting research to develop a theoretical framework, two realms exist – observation and theory. The researcher is required to work between these two realms to express their beliefs and ideas with regard to the phenomena that are being studied (Trochim & Donelly, 2006). Furthermore, a theoretical framework brings justification to the overall research (Maxwell, 2005).

5.4.2 Types

Conceptual frameworks are close to empirical inquiry and can take different forms depending on the research problem and the questions they need to address. Several types of conceptual framework include working hypotheses, descriptive categories, practical ideal types and methods of research, and formal hypotheses (Oates, 2006). These types of frameworks are associated with particular research purposes, such as exploration, description, quantitative analysis and qualitative analysis. The alignment of framework and purpose makes other aspects of empirical research more obvious. These include the choice of methodology and data analysis techniques.

Existing theory and relevant research are influential for developing a conceptual framework, since they facilitate the understanding of the phenomena that are under investigation (Maxwell, 2005). The purpose of constructing a framework is both descriptive and critical: it will provide the researcher with the ability to understand and communicate problems and gaps that are identified in current theory and research and it makes the original contribution of the study more evident to comprehend.

The purpose of this study is to develop a framework to evaluate USec in online social networking. It is based on a descriptive type of conceptual framework that explores the fields of HCI, InfoSec and USec and utilises qualitative and quantitative methods. The findings from the methods are aligned in a framework to evaluate USec.

5.4.3 Typical Components

Figure 5.8 illustrates the composition of a framework. Lethbridge and Laganiere (2005) portray it as process that moves between three cycles. At the first cycle, the components of interest, which are the main focus areas of the research, are identified. Thereafter, the process moves to the second cycle. At this point, various components are integrated by determining the relationships that connect them. Once all these relationships have been identified, the process can move to the third and final cycle; the actual framework. This will include all the components along with their relationships. However, in this cycle they comprise one logical unit.

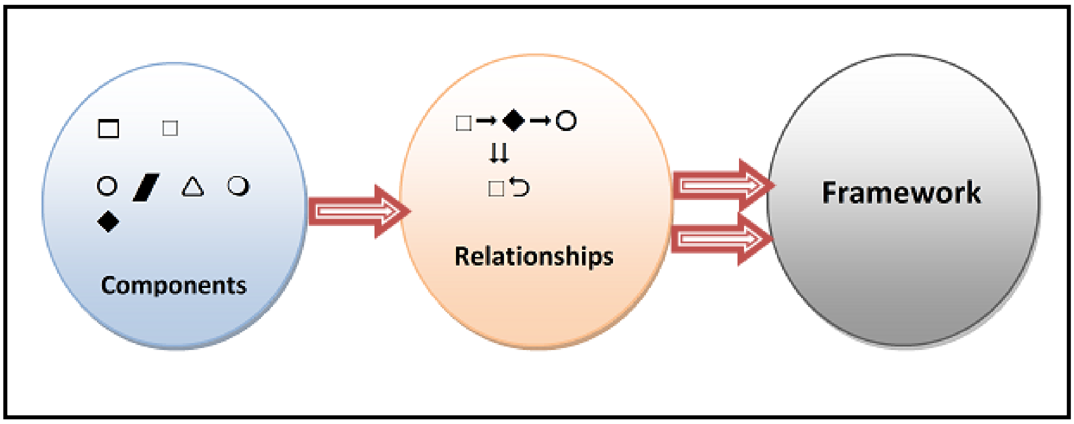


Figure 5.8: The composition of a framework (Lethbridge & Laganiere, 2005)

5.5 RESEARCH METHODS AND DESIGN FOR THE STUDY

This section discusses the research model for the study. The research questions, primary and sub, will also be mentioned once again.

5.5.1 Research Questions

The primary research question is:

What are the components of a framework to qualitatively evaluate usable security?

The main research question gives rise to a number of sub-questions. These will need to be addressed first and include:

1. *Which usability inspection method can be adapted to evaluate usable security?*
2. *Which approach can be followed to develop the method?*
3. *How can the validity and applicability of the method and approach be tested?*
4. *How can the method and approach be constituted into a framework?*

5.5.2 Research Paradigm

Based on the overview of the paradigms in section 5.2.1, it is concluded that there is lack of consensus regarding HCI research (Ford, 2005; Van Greunen 2009). Consequently, it has become common practice to implement a combination of quantitative and qualitative strategies in HCI research. By considering this factor and by investigating the various HCI research paradigms, this research is based on the fundamental ideas that support the engineering paradigm, as discussed in section 5.2.1.3.

There are two main reasons for maintaining the need to implement an engineering paradigm. However, that being said, the other paradigms should not be devalued or underestimated. It is in accordance to the nature of this research that the engineering paradigm is considered to be more efficient and suitable for answering the primary research question. The two reasons supporting its implementation include:

1. It was previously stated that there are established and non-established paradigms. In order to avoid criticism, the preferred option would be to implement an established paradigm instead of a newly proposed or non-established paradigm. Defending a non-established paradigm could impose further difficulties and require consensus, which is difficult to achieve even with the established paradigms.
2. By comparing the various established paradigms that make use of quantitative and qualitative strategies, the one that is based on developing knowledge by examining interface design is engineering.

5.5.3 Research Philosophy

The research philosophy and related methodologies to be followed in this study are based on an interpretivist approach, as discussed in section 5.3.1.2. This philosophy is well suited for this type of research because the main focus is to observe the patterns and behaviours of users interacting with security and privacy in OHSNs.

Based on the philosophy, there are concerns regarding research bias. The foremost concern relates to the stance of the researcher in terms of the two fields being examined, usability and security. As mentioned, the study resides in the HCI field, so it leans more towards the usability component. In order to avoid bias, other perspectives are considered. The opinions and preferences of individuals purely from the InfoSec field (represents the security component) and HCI field alike will be independently considered. In addition, the opinions of a third perspective will also be examined. These are individuals from the USec field, whose knowledge crosses both fields, usability and security, and therefore have adopted a more USec perspective.

Collecting and analysing data from the three fields, HCI, InfoSec, and USec, will provide a wealth of information. Combining this information and extracting the most useful aspects of it will assist in the development of the USec framework for online social network environments.

5.5.4 Research Approach

The research approach will be based on inductive reasoning, as discussed in section 5.3.2.2. Accordingly, the final step will be the development of some general conclusions or theories in the form of a framework for USec. In essence, the particular literature will be analysed by identifying patterns, themes and regularities (Trochim & Donelly, 2006). Examining these patterns will ultimately assist in the development of new theory.

5.5.5 Research Strategy

In terms of the research method, it has to be determined which research strategy is better suited for this study. To decide this, a technique was adapted from the research of Van Greunen (2009) and Van der Merwe, Kotze and Cronje (2005). This technique matches the four research sub-questions against the characteristics of the four research strategies that were discussed in section 5.3.3. The results are displayed in table 5.3.

Table 5.3: Research strategy characteristics and the research questions
(adapted from Van Greunen, 2009; Van der Merwe et al., 2005)

Research strategy	**Characteristics**	**Sub-question 1**	**Sub-question 2**	**Sub-question 3**	**Sub-question 4**
Case study	Investigator has little control	√	√	√	√
	Contemporary phenomenon in real-life context	√	√	√	√
	Explores a single entity or phenomenon bounded by time and activity		√	√	√
	Study life cycles	√	√	√	√
Ethnography	Active participation		√	√	
	Observational data				
	Social contact with participants				
	Extended depth study	√	√		
	Limited to one field study				
Survey	Aimed at producing reliable statistics on specific issue			√	
	Description of data			√	

Research strategy	**Characteristics**	**Sub-question 1**	**Sub-question 2**	**Sub-question 3**	**Sub-question 4**
	characteristics				
	Used to identify cause based on data				
Action research	Focuses on what participants do			√	
	Explicit criteria				
	Practitioners and researchers with mutual goals				
	Apply theory with goal to enhance	√	√		

The results of the evaluation of the sub-questions against the research strategies' characteristics confirm that this research study can be characterised as a case study problem. The case study follows an interpretivist research philosophy to develop a framework for evaluating USec. A case study, as was discussed in section 5.3.3.1, is a useful technique for extracting a wealth of information about specific subjects and it offers multiple purposes. Most importantly, it provides the platform for testing the process to develop heuristics for SADs. This process is then subsequently applied to developing heuristics for the domain of USec. By implementing the case study, the USec HE will also be improved. The data collection and analysis techniques to support the case study are discussed in sections 5.5.8 and 5.5.9 respectively.

The case study also serves to evaluate OHSNs. For this, two subjects are used: MedHelp and Google Health. The case studies will offer a holistic portrayal and representation of the users' experiences when interacting with the OHSNs. Interactions of particular interest are those relating to security-related tasks. Such interactions will help evaluate the effectiveness of the security, by identifying its strengths and weaknesses in terms of usability. The identification of its successes and failures will provide a wide range of constructive information, which can then be analysed.

Based on the analysis of the process application, the evaluation of the USec HE and the examination of the OHSNs, patterns in the data will emerge. Once all the data have been collected, further analysis will be carried out. Patton (1990) states that the results of the case study should improve the overall system, once the appropriate changes have been recommended and implemented. Similarly, the results from the case study in this research will demonstrate the applicability of the process for developing heuristics for SADs and improving the USec HE. In this research, recommendations will only be made to improve the USec of the OHSNs.

The purpose of the data gathered from case studies is to reveal and evaluate theories resulting from the differences that have been observed. Furthermore, the effectiveness of interaction theory can be demonstrated to the implementers themselves (Markus, 1983; Van Greunen, 2009). Six steps for case study research have been proposed by various researches (Yin, 2008; Soy, 1997). The six steps have been adapted to the context of this research in table 5.4.

Table 5.4: Implementing Soy's six steps of case study research in this study (Soy, 1997)

Steps		Guidelines for the researcher
1	Determine and define the research questions	Primary and sub research questions are displayed in section 5.5.1.
2	Select the cases and determine data gathering and data analysis techniques	A case study will be applied to develop a USec HE by implementing the process to develop heuristics for SADs. A case study will also be conducted on two OHSNs. Data gathering techniques include secondary data, FUE, HE and questionnaires. Data analysis techniques include theme analysis and descriptive statistics.
3	Prepare to collect the data	Pilot studies will be conducted in order to remove any problems with the FUE scripts. Participants will then need to be identified and letters of introduction created. Rules for confidentiality must also be established. For the HE with experts, a tool must be developed to validate the USec HE. Experts from the field of InfoSec, HCI and USec must then be identified. Letters must be provided explaining the purpose of the HE and how their assistance is required.
4	Collect data in the field	All sources of data must be sorted in a format that can be analysed. All documents from the FUE with users and the HE of experts with the validation tool are in Word or Excel documents. Comments are also provided on both. The data should provide a means to identify patterns within them. Keep participants and experts informed about the course of the study and the data as the study progresses. Therefore, if there is a need to have additional meetings with the participants or experts it can be arranged.
5	Evaluate and analyse the data	By identifying patterns within the data, it is possible to answer the questions defined in step 1. Linkages can be identified in the raw data of the various data gathering techniques. Data triangulation will be applied to strengthen the research findings.
6	Prepare the report	Complex data must be reported in a form that can be understood by readers. The main source of report will be the thesis. Additional forms of report will include papers for conferences and articles for journals.

5.5.6 Research Choices

The research choice will be based on mixed methods; hence employing a mixed-model research choice, as discussed in section 5.3.4. This model implies the use of quantitative and qualitative data collection techniques for analysis. A critical aspect of this model is that the quantitative and qualitative techniques are used in combination and not in sequential order. Both quantitative and qualitative data will be collected by means of the questionnaires and HE. Moreover, qualitative data will also result from the overall case study and from the experts' validations and the participants' formative usability evaluations (FUEs). The manner in which the quantitative and qualitative data collected from the mixed-model research choice will be analysed is mentioned in more detail in section 5.5.9.2.

5.5.7 Time Horizons

A longitudinal study, as discussed in section 5.3.5.2, will be preferred, as the study will be completed over an extended period of time. Specifically, the research must be completed within a period of three years. The purpose of the research is to develop a USec framework. This will require an analysis of OHSNs and USec theories over longer periods of time (Saunders et al., 2000).

5.5.8 Data Collection Techniques

All selected techniques will contribute to the success of this research and will assist with the collection of the required information. A combination of qualitative and quantitative data collection techniques will be applied. These include secondary data (as discussed in section 5.3.6.1), questionnaires (as discussed in section 5.3.6.5), FUE and HE (as were discussed in section 5.3.6.6). Figure 5.9 displays the research onion model that will be implemented and which has been adapted from the original version of the research onion model (displayed in figure 5.1) in order to accommodate this specific research study. All six levels of the model are displayed, along with their selected options. In the following sections the data collections techniques are discussed.

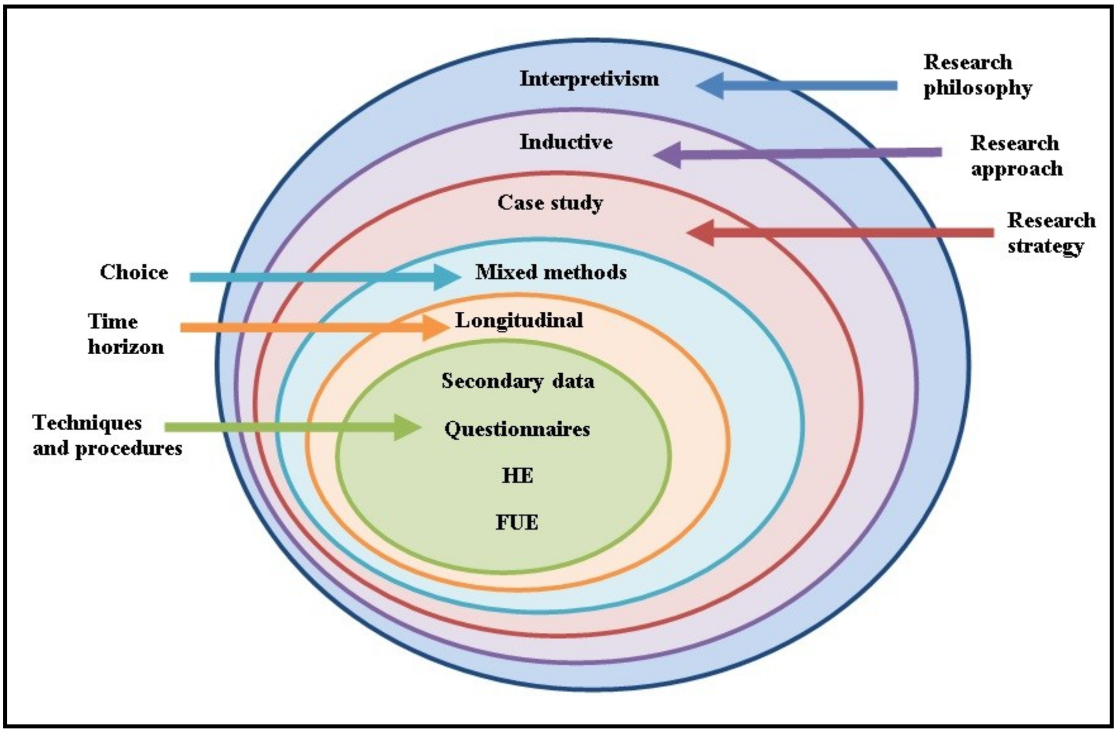


Figure 5.9: The research onion model to be applied for this study

5.5.8.1 Secondary Data (Literature Review)

The literature review will be based on the examination of relevant papers, journal articles, white papers, and books. The Internet will provide a platform on which much of the literature will be found. This literature will relate to the fields of USec, HCI, InfoSec, OHSNs and frameworks.

5.5.8.2 Questionnaires

Questionnaires are used to extract certain information from the participants. They will be used in the form of user satisfaction questionnaires in the FUE and in the validation tool that experts will use to assess the USec HE. The purpose is to determine participant and expert satisfaction with regard to the application and usage of the USec HE.

5.5.8.3 Formative Usability Evaluation

The purpose of the FUE is to collect data while participants perform security-related tasks on the OHSNs. In this case, they will be provided with scenarios and tasks. An FUE is used because the OHSNs are already developed. If the system were new, a different type of evaluation technique would be used to collect the user requirements. It is important to clarify that the FUE does not investigate the overall UX on the selected OHSNs. For that reason usability metrics are not considered in the evaluation, but are used when evaluating the performance of participants against tasks using quantitative measures. The focus is purely on testing the USec HE in context. The feedback received is the outcome of the security and privacy tasks that the participants performed on the websites. Based on this feedback, recommendations are made to improve the level of USec for the selected OHSNs.

In this research, the participants who conducted the FUE were postgraduate students. More detail on the participants and the scenarios and tasks they conducted is provided in chapter 6. This section will focus on the development of criteria to select the OHSNs for the case study and the procedure that was followed to implement them.

There are many OHSNs on the Web that offer different functionalities and services, as will be discussed in chapter 6. Therefore, an important consideration for the FUE was to determine the key components of OHSNs in order to select the most appropriate OHSNs for the case study. This will ensure that the websites selected for the case study adhere to specific requirements. The requirements for selection were determined on the basis of four sets of requirements; each comprising its own criteria. The four sets include

- social networking components
- health application domain
- scope of functionality
- supplementary factors

Social networking components

In order for websites to be considered as social networking tools, it is necessary that they contain certain architectural components. These architectural components are assesses as being commonly accepted practices and provide a template for the baseline criteria of social network sites. The minimum key characteristics that are identified and which need to be incorporated into such websites include (Boyd & Ellison, 2007):

- *Profile*. This will need to be visible and within a bounded system. It is used to describe the actor (user).
- *Connections*. This includes both public and semi-public connections. These connections will be between the actor (a profile representing the particular actor) and his/hers relations (e.g. friends, employees etc.).

- *Navigate*. This relates to the navigation of the actual connections. Users that have profiles should also have the ability to traverse their connections (e.g. view their connections' profiles or pictures).

The Burton Group expanded on the minimum key characteristics identified by Boyd and Ellison (2007) and included additional capabilities as criteria as well. They suggest that these capabilities should also be considered as core functions of a social network site. The additional capabilities include the following (Gotta, 2008; Hogben, 2007):

- *Multiple means for connections*. There must be alternative means for members to participate, interact and contact a particular actor (e.g. e-mail, instant messaging, chat rooms etc.). These tools also provide a platform for posting personal data on a profile (e.g. the actor's personal interests).
- *Visibility controls*. The actor should have the ability to manage his/her own visibility, via a set of controls (e.g. search, profile viewing etc.).
- *Tools for interaction*. The actor should have the ability to manage the manner in which they prefer to interact or to be contacted by other members, via a set of controls (e.g. messages). These tools provide personalised, socially-focused interactions that are based around the profile (e.g. recommendations, reports of events etc.).
- *Access controls*. These are tools that are used to define social relationships and to determine permissions as to who has access to the actor's data via their profile and as to who can communicate with the actor.

The attributes discussed above, in the form of key characteristics and additional capabilities will need to be mapped onto the architectural components of profiles, social graphs, participation models, social presence and relation controls. This will assist all the related parties (e.g. application developers, infrastructure planners etc.) in designing a social network website (Gotta, 2008). Figure 5.10 displays the architectural template of a social network website.

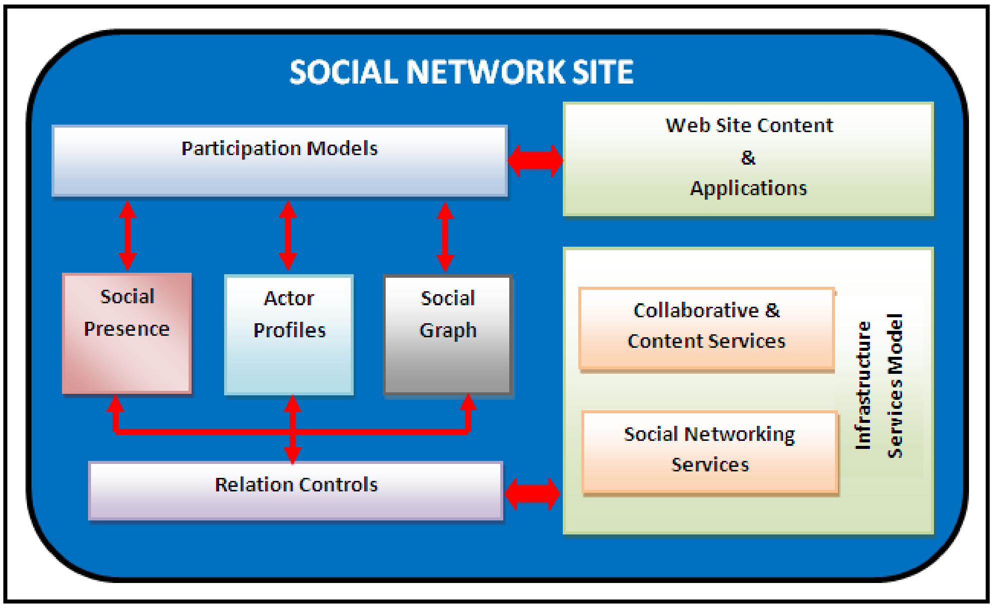

SOCIAL NETWORK SITE
Participation Models
Web Site Content & Applications
Social Presence
Actor Profiles
Social Graph
Collaborative & Content Services
Social Networking Services
Infrastructure Services Model
Relation Controls

Figure 5.10: The architectural components of a social network website (Gotta, 2008)

Health application domain

The second requirement is focused on defining the application domain of the site, in this case, with regard to its health context. Several criteria are identified, in which one may define the health application domain of OHSNs:

- *Free-standing or integrated.* Free-standing would refer to an autonomous health website. An example of such a site is SugarStats. Although a patient may share their personal health information with their health care provider, it is not necessary for the health care provider to have any particular system in its own premise to view or analyse that information. Instead, integrated refers to a health website that is also incorporated into a system that is owned by the health care provider. Thus, it has the capabilities to import and export medical information from different sources (Alder, 2006). Integrated sites provide patients with more options when interacting with their health care providers. In addition, they allow them to take their information with them when changing health care providers. In addition, they also provide for networking with other patients. Google Health can be categorised as an integrated site. However, the integration in this case is done via third-party companies. Patients are able to import their medical health records into Google Health through a third-party site, such as Allscripts. This would entail that the health care provider has an Electronic Medical Record solution in place (e.g. Allscripts Professional). The networking between the health care providers and their patients would then happen through the Allscripts Professional Patient Portal.

- *Patient-specific or health care provider-specific*. This distinguishes the sites users as either being health care providers or patients. An example of a health care provider's site is Sermo, while an example of a patient-specific site is PatientsLikeMe. There is also the possibility that a health social network site accommodates both the patients and the health care providers. In this research, such a site is defined as a hybrid-specific site and an example of it would be MDLinked.
- *General health or disease-specific*. In this context, disease specific refers to a site targeting patients suffering from a specific disease. An example of a disease-specific site is I'm too young for this! cancer foundation. This site targets patients suffering from cancer or those who seek cancer-related information or help. In contrast, *general health site* refers to a site that caters for a number of different conditions or symptoms, one example being Daily Strength. This site offers multiple and diverse support groups.

Scope of functionality

To determine the conditions to select the OHSNs for the case study, an additional requirement needs to be considered. This focuses on the actual scope of functionality that is provided by the website. These are functionalities associated more with the health social networks, unlike the first requirement, which discusses key characteristics and components of general social network sites. These functionalities can contribute significantly to the development of good health social network site. However, some of the functionalities will not be available in other general online social network environments. These include the following (Boulos & Wheelert, 2007; Purdy, 2008; Hughes, Joshi, & Wareham, 2008; Eysenbach, 2008):

- The website must empower end-user participation. It needs to provide the abilities to facilitate participation from the respective end-users. This should be either the patients, caregivers, health care providers or all three user types.
- The website must provide ongoing medical education and information regarding the area of focus (e.g. OHSNs for cancer patients should provide the analogous medical information and education regarding cancer).
- The website must instil trust to the users. This is achieved by considering security and privacy issues with Web 2.0 services. Credible information on the website also has a

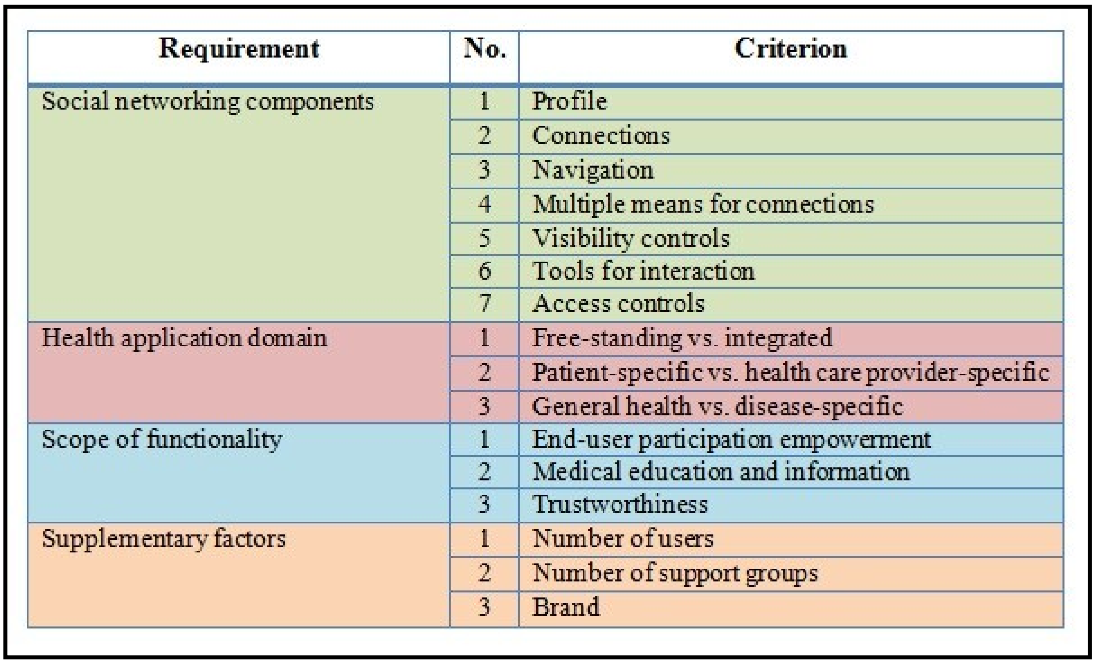
significant role to play in contributing to trustworthiness. This is important in the context of health social network sites where shared patient information intrinsically requires proper protection.

Supplementary factors

This set may be debated as to whether it justifies the principle of a requirement. However, it can have an impact in the selection process. For this reason alone it has been accepted and defined as one of the requirements, which are discussed in the form of supplementary factors. These factors are the following:

- *Number of users* – a site with more members would be more popular and its features would have been utilised more than those of unpopular sites.
- *Number of support groups* – a site with a larger number of support groups would incidentally attract a higher number of users.
- *Brand* – the name of the site or the organisation which owns the health site could also be an influential factor (e.g. Google Health and MS HealthVault).

To summarise, four sets of baseline requirements have been determined; social networking components, health application domain, scope of functionality and supplementary factors. These requirements are used as a template for selecting the OHSNs for the case study. The websites will then be assessed by means of the USec HE. The requirements to be used, as well as their criteria, are displayed in figure 5.11.



Requirement	No.	Criterion
Social networking components	1	Profile
	2	Connections
	3	Navigation
	4	Multiple means for connections
	5	Visibility controls
	6	Tools for interaction
	7	Access controls
Health application domain	1	Free-standing vs. integrated
	2	Patient-specific vs. health care provider-specific
	3	General health vs. disease-specific
Scope of functionality	1	End-user participation empowerment
	2	Medical education and information
	3	Trustworthiness
Supplementary factors	1	Number of users
	2	Number of support groups
	3	Brand

Figure 5.11: The requirements to select the OHSNs for the case study

Figure 5.11 displays the four requirements and their criteria, which were used to select the OHSNs for the case study. The purpose is to identify which of the criteria for each requirement are apparent on the site. In the case of the health application domain requirement, the purpose is to determine the type of health site. In essence, each criterion will be associated with a specific weight or value. The sites with the highest accumulated values will be the ones selected for the case study. This is necessary because a plethora of OHSNs exist. Once evaluated by the criteria, the websites will be determined. The OHSNs to be considered are displayed in table 5.5 and figure 5.12.

Table 5.5: Possible OHSNs that will be evaluated by the specified requirements

OHSNs/URL	OHSNs/URL
Daily Strength: www.dailystrength.org	TuDiabetes: www.tudiabetes.org
Healthline: www.healthline.com	WEGO health: www.wegohealth.com
Healia: http://communities.healia.com	Keas: www.keas.com
Cochlear Community: www.cochlearcommunity.com	Wellsphere: www.wellsphere.com
Hope Cube: www.hopecube.com	Google Health: www.google.com/health/
Icyou: www.icyou.com	Microsoft HealthVault: www.healthvault.com
iMedix: www.imedix.com	PatientsLikeMe: www.patientslikeme.com
MDJunction.com: www.mdjunction.com	Sermo: www.sermo.com
I’m too young for this! cancer foundation: http://i2y.com	MDLinked: www.mdlinked.com/
MedHelp: www.medhelp.org	Medscape Physician Connect: www.medscape.com/connect
SugarStats: www.sugarstats.com	

Figure 5.12: Logos of the OHSNs

Procedure for selection

Since the requirements for selecting OHSNs have been defined, a procedure must now be followed to implement them. The procedure for selecting the websites was based on four stages. These include the following:

- *Stage 1 – Research and literature review*. A background literature review was conducted in the fields of online social networking environments and OHSNs specifically. This resulted in identifying characteristics and components for these types of website. The investigation also assisted in identifying a total of twenty-one possible websites for selection. These are displayed in table 5.6.

- *Stage 2 – Development and application of extensive set of requirements*. To determine which of the twenty-one websites were appropriate for the case study, an extensive set of requirements was established. These requirements were based on work conducted in Stage 1 and were specific to the health context. Requirements were then categorised under four main groups; Social Networking Components, Health Application Domain, Scope of Functionality and Supplementary Factors. Thereafter, a three-point rating scale was used to determine the level of conformance of a website with regard to each requirement. The measurements for the three-point rating scale were defined as the following:
    - 0 = does not satisfy requirement

  - 1 = moderately satisfies requirement
  - 2 = fully satisfies requirement

  An example illustrating the difference between a scale 1 and a scale 2 rating is provided. One requirement states that "*The user can express personal relationships by establishing various types of connections (e.g. with other patients, friends, family or doctors)*". If a website were provided with a scale 1 rating for this requirement, it entails that a user may establish a relationship with a single type of connection only. A scale 2 rating would entail that the user can establish relationships with several type of connections. Evidently, a scale 0 rating entails that the user is not able to establish any relationships on a website. By applying the extensive set of requirements in this stage, it was possible to eliminate six websites for various reasons. The application of the extensive set of requirements is presented in *Appendix D.1: Extensive Set of Requirements*. This result, a total of fifteen possible websites could now be assessed for selection in Stage 3.

- *Stage 3 – Development and application of minimum set of requirements*. Once all the websites had been measured against the extensive set of requirements in Stage 2, a set of minimum requirements was established. These were derived from the extensive set of requirements, yet were marginally modified. Determining what the minimum requirements were was grounded on defining the type of website that would be more suitable to evaluate with the USec HE. This mostly depended on the features available and the target audience of a website. The purpose of the minimum requirements was to further eliminate websites in order to determine the two that would be selected for the case study. This process was aided by the fact that all websites had already been measured against the extensive set of requirements of the previous stage. It was consequently easier to determine if a website adhered or not to a minimum requirement. A total of eight minimum requirements were established. The application of the minimum set of requirements is presented in *Appendix D.2: Minimum and Bonus Set of Requirements*. For a website to be considered for selection in the case study, it had to adhere to all of the minimum requirements. In addition to the minimum requirements, two bonus requirements were also established. These would only be considered in a case where more than two websites adhered to all the minimum requirements. At this stage, eight websites were eliminated. As a result, a total of seven possible websites could now be assessed for final selection in Stage 4.

- *Stage 4 – Application of bonus requirements*. A total of seven websites adhered to all of the minimum requirements in Stage 3. Therefore, the bonus requirements were then considered. The application of the bonus set of requirements is presented in *Appendix D.2: Minimum and Bonus Set of Requirements*. Only two of the seven websites adhered to both of the bonus requirements, however. Therefore, they were automatically selected for the case study. These were MedHelp and Google Health.

- If more than two websites had adhered to the bonus requirements then supplementary factors from figure 5.11 would have been considered (e.g. the two websites with the most registered users are selected for the case study).

Figure 5.13 displays the four stages in the procedure to select the OHSNs for the case study. It also displays those that were eliminated at each stage. These can be identified by the red rounded rectangles surrounding them. The selected OHSNs are identified by the green rounded rectangles surrounding them.

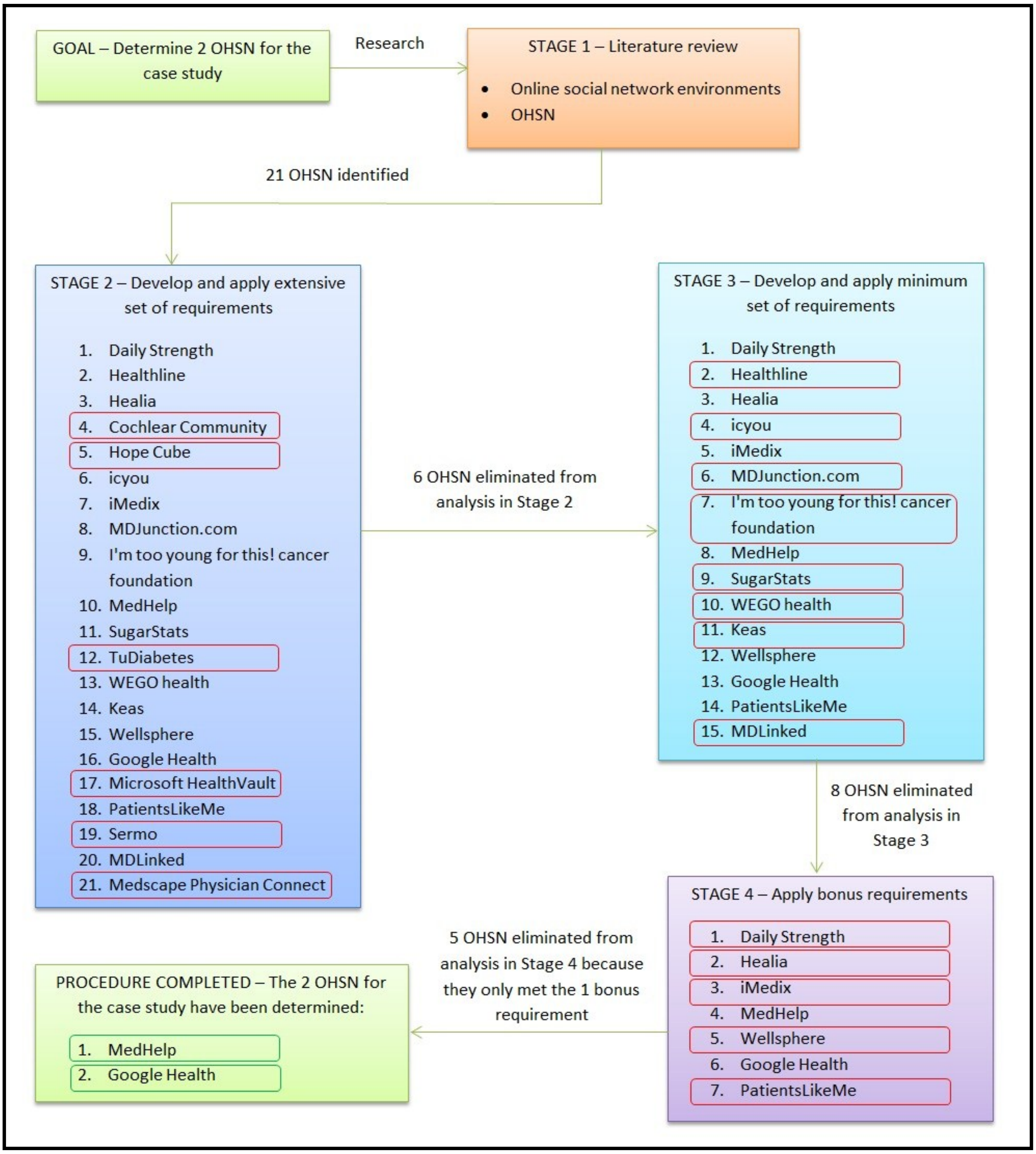

GOAL – Determine 2 OHSN for the case study
Research
STAGE 1 – Literature review
Online social network environments
OHSN
21 OHSN identified
STAGE 2 – Develop and apply extensive set of requirements
1. Daily Strength
2. Healthline
3. Healia
4. Cochlear Community
5. Hope Cube
6. icyou
7. iMedix
8. MDJunction.com
9. I'm too young for this! cancer foundation
10. MedHelp
11. SugarStats
12. TuDiabetes
13. WEGO health
14. Keas
15. Wellsphere
16. Google Health
17. Microsoft HealthVault
18. PatientsLikeMe
19. Sermo
20. MDLinked
21. Medscape Physician Connect
6 OHSN eliminated from analysis in Stage 2
STAGE 3 – Develop and apply minimum set of requirements
1. Daily Strength
2. Healthline
3. Healia
4. icyou
5. iMedix
6. MDJunction.com
7. I'm too young for this! cancer foundation
8. MedHelp
9. SugarStats
10. WEGO health
11. Keas
12. Wellsphere
13. Google Health
14. PatientsLikeMe
15. MDLinked
8 OHSN eliminated from analysis in Stage 3
STAGE 4 – Apply bonus requirements
1. Daily Strength
2. Healia
3. iMedix
4. MedHelp
5. Wellsphere
6. Google Health
7. PatientsLikeMe
5 OHSN eliminated from analysis in Stage 4 because they only met the 1 bonus requirement
PROCEDURE COMPLETED – The 2 OHSN for the case study have been determined:
1. MedHelp
2. Google Health

Figure 5.13: The four-stage procedure for selecting the OHSNs for the case study

5.5.8.4 Heuristic Evaluation

The USec HE was used by users in the FUE to experience its usage and application. Their views were then collected using the user satisfaction questionnaires, which made it possible to determine whether the USec HE is successful in evaluating the level of USec on the OHSNs. It is then possible to make recommendations to improve the security and privacy features that are lacking from a usability point of view.

The USec HE was also reviewed by experts using a validation tool, which was developed in this study. The validation tool examined the heuristics and their related checklist items for USec. It also assessed two new sets of USec severity ratings and the material considered to develop the heuristics and checklist items. It also included a user satisfaction questionnaire to measure the experts' views with regard to the overall USec HE.

The validation of the USec HE was conducted by experts from the fields of HCI, InfoSec and USec. Seven experts agreed to participate in the validation; of these four returned their assessments by the cut-off date and one did not complete the entire validation tool. Of the four experts, two were from InfoSec, one from HCI and one from USec. The panel of experts are representative of the related fields and the one from USec brings knowledge of HCI and InfoSec as well. Two of the experts were international and two were local.

There are very few experts in the field of USec, making it difficult to find participants. Usually, these tend to be experts in the field of InfoSec, who understand and appreciate the importance of HCI. They have a basic understanding of the HCI field although their background remains InfoSec. However, selected experts have conducted research in both fields and can be classified as USec experts. These are the experts that we classify as USec experts in this study. The USec expert that participated in the validation is representative of such a group.

5.5.9 Data Analysis Techniques

Data analysis techniques assisted in analysing the data collected using the various data collection techniques. The two data analysis techniques that are used in this research study are theme analysis and descriptive statistics.

5.5.9.1 Theme Analysis

Data analysis in qualitative research is ongoing throughout the data collection process. It requires that the researcher constantly thinks and reflects on emerging themes, and then adapts and changes methods if needed.

Thematic analysis was used to develop the USec HE. Based on the literature review of the USec, HCI and InfoSec fields, key themes were identified. These themes represented the main requirements of security and usability and were subsequently transformed into heuristics for USec. Within these resided their related checklist items. The themes are presented in section 4.4.1. Their transformation into high-level heuristics with checklist items for USec was discussed in detail in sections 4.4.2, 4.4.3 and 4.4.4.

As soon as the results from the case study were collected, an exploratory analysis of the data was made before the actual data analysis process began. This provided the capacity to make more sense of the diverse information. To support this, the data collected were in a format that could be easily analysed.

In the FUE, the results of the scenarios and tasks that participants conducted were in Word format. The HE that they conducted on the two OHSNs and the user satisfaction questionnaires they completed were also in Word format. At the end of the FUE, participants compared the two OHSNs and the results were recorded in Excel spread sheets. The FUE facilitated the process of determining usability shortcomings, concerning security and privacy features in OHSNs. When the issues have been resolved, it is then possible to provide recommendations for addressing the identified problems (Barnum, 2002). Additionally, once this process is complete, key information will have resulted that can contribute to the development of the OHSNs with improved USec. The results and analysis of the FUE are discussed in section 6.3.

The experts assessed the USec HE with a validation tool. The validation tool was developed in Excel and included seven sheets. The results obtained from applying the validation tool are presented in chapter 7. The tool itself is described in section 8.4.

5.5.9.2 Descriptive Statistics

For the purpose of this research, descriptive statistics are used to summarise and explain the data. The methods that will be used for the descriptive statistics include graphs and frequency tables. Frequency tables are the simplest method by which one may represent categorical and ordinal data and are commonly used as an exploratory procedure when attempting to establish how the different categories of values are distributed within the sample.

In the FUE, frequency tables were used to summarise the responses of the participants as frequency counts. This occurred where the security and privacy features of the two OHSNs were measured against usability criteria in section 6.3.1.4.1. It also occurred in section 6.3.1.4.2 where the tasks that the participants performed were measured against USec ratings. Frequency counts were also used to summarise the participants' responses in the user satisfaction questionnaires. These are presented in section 6.3.3. Graphs were used in the form of column charts. In section 6.3.1.4.1 these were used to compare the results obtained from evaluating the usability of security and privacy features of both OHSNs. Column charts were also used in section 6.3.1.4.2 to compare the results obtained from evaluating the level of USec when performing tasks on both OHSNs.

To analyse the results obtained by the validation tool, frequency tables and graphs were again implemented. Frequency counts were used to express the experts' ratings in terms of the importance and clarity of the USec high-level heuristics in section 7.2.3. Two sets of USec severity ratings were examined in section 7.2.5 and frequency tables are used to express the experts' ratings in terms of the ease of application and relevance of both sets. In section 7.2.6 the material that was used to develop the USec HE is assessed. Frequency counts are used to measure the novelty and relevance of usability and USec material and security and privacy material. Frequency counts were also used to summarise the experts' responses in the user satisfaction questionnaires.

Graphs in the form of column charts were used. In section 7.2.3, two column charts were used: the first represented a comparison of expert ratings regarding the level of importance of each USec heuristic and the second a comparison regarding their level of clarity. In section 7.2.4.13 a column chart is used to display the checklist items that provided low ratings when measured against a set of criteria. The results represent the experts' responses in terms of frequency counts and percentages.

5.6 DATA TRIANGULATION

Data triangulation requires the use of multiple sampling strategies to collect data with the purpose of obtaining it from different times, social situations and people. Denzin (1970) states that data triangulation is only one form of triangulation. The other forms are theoretical triangulation, investigator triangulation and methodological triangulation. Theoretical triangulation requires the use of more than one theoretical position when interpreting data, while investigator triangulation requires more than one researcher to gather and interpret data and methodological triangulation requires the use of multiple methods for gathering data, thus is also referred to as multi-method, mixed-method, or methods triangulation. Thurmond (2001) also lists data-analysis triangulation as another form that requires multiple methods for analysing data. In terms of this research study, the forms of triangulation that will be applied include data triangulation, methodological triangulation and data-analysis triangulation.

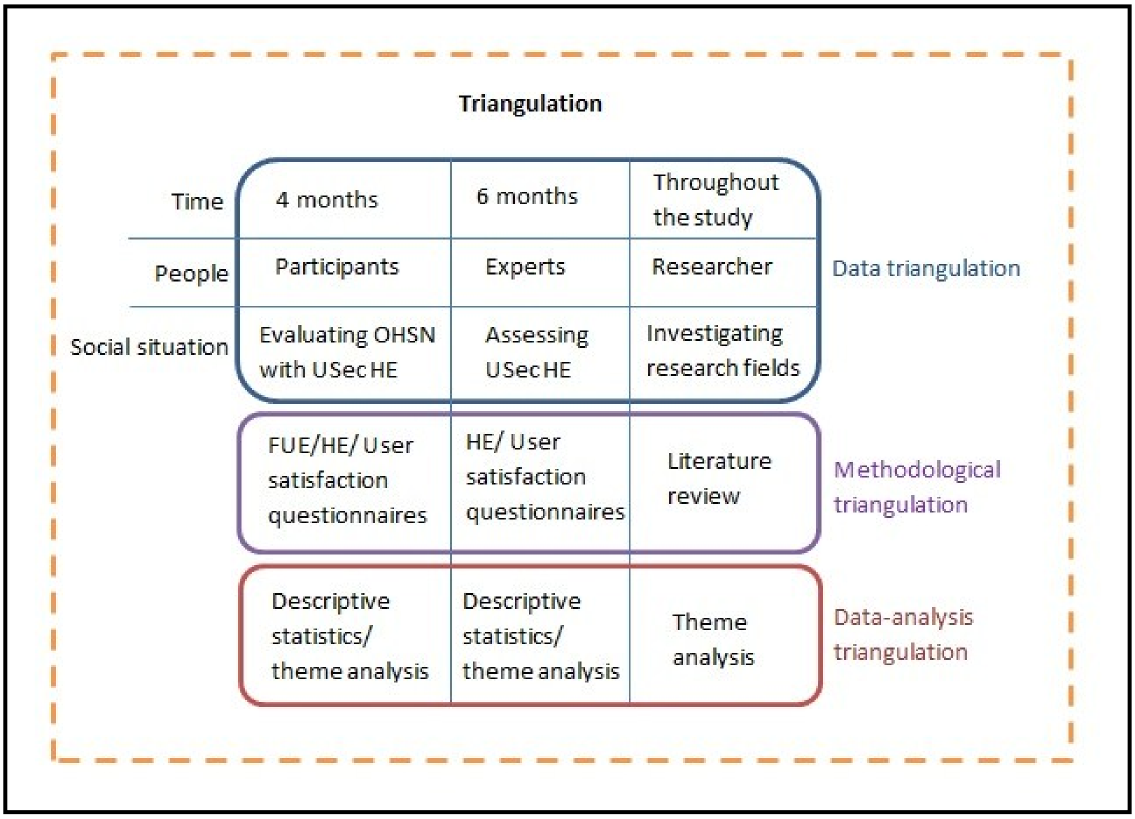
Data triangulation is defined as the combination of strategies in an attempt to study the same phenomenon. It ensures that the inconsistencies reflected are due to trait rather than actual research strategy. Results will then be valid and not the outcome of a methodological artefact (Jick, 1979). When combining primary data (data collected by researchers themselves) and secondary data (data collected from other resources) the outcome is data triangulation. This provides one with the opportunity to validate findings by applying several different research methods. This will in turn enhance the credibility of the findings (Driscoll, 2006).

Reliability and validity of data are elemental for successful research. To achieve reliability, the data need to be consistent, precise and repeatable. Otherwise, the derived conclusions will be worthless. The same applies for invalid data, which will be of no value because it provides a fake representation of a social reality. Consequently, it does not provide a true measurement of what is actually occurring in society. Data triangulation provides one with the ability to instil the concepts of reliability and validity in their data. In addition, it offers the opportunity to only utilise strong points of different data collection techniques, before integrating them to collect the data. Furthermore, data triangulation promotes productive research. That being said, there are cases where data triangulation is not deemed suitable. This is due to constraints, such as cost and time (Jick, 1979).

The research is subject to methodological triangulation as well because it combines quantitative and qualitative data collection techniques. The consensus is that quantitative and qualitative research techniques are used collectively because they complement each other, instead of rivalling one another (Jick, 1979). In the regard, Hofstee (2008) mentions that quantitative techniques are used to measure the relationship between two or more items in a statistical format. When evaluating the relationship quality between two or more items, qualitative techniques are employed because they assist the researcher to make sense of people’s interpretations and understandings.

Applying multiple data collection techniques within a single research study is well supported, yet it requires considerable preparation. Selecting the appropriate methods and combining them effectively requires great thought. This is critical for successful triangulation and will assist in the better convergence and interpretation of the data, which in turn will result in more clear and credible data. The data collection techniques or methods, as they are referred to in this form of triangulation, are literature review, FUE, user satisfaction questionnaires and HE. The reasons for selecting these and the way they were individually applied, is elaborated on in section 5.5.8.

Lastly, the data collected from applying methodological triangulation must be quantitatively and qualitatively analysed. Hence, the data are subjected to data-analysis triangulation. In considering the data collection methods that were applied, descriptive statistics and theme analysis will be used to analyse and interpret the data, as discussed in section 5.5.9. With regards to this research, the forms of triangulation – data, methodological and data-analysis – are suitable and demonstrate the reliability and validity of the collected data. Figure 5.14 displays how the three forms of triangulation combine, in an attempt to collect more reliable and valid data. They are integrated to represent the triangulation process and to demonstrate their convergence.



Triangulation

Time	4 months	6 months	Throughout the study	Data triangulation
People	Participants	Experts	Researcher	
Social situation	Evaluating OHSN with USecHE	Assessing USecHE	Investigating research fields	
	FUE/HE/ User satisfaction questionnaires	HE/ User satisfaction questionnaires	Literature review	Methodological triangulation
	Descriptive statistics/ theme analysis	Descriptive statistics/ theme analysis	Theme analysis	Data-analysis triangulation

Figure 5.14: The convergence of the three forms of triangulation

As shown in figure 5.14, it is noticeable that the data triangulation is divided into time, people and social situation. These are explained in terms of the three cases to which they were applied. Time represents the total period required to prepare, conduct and analyse the case. The methodological triangulation shows the data collection techniques that were applied for each case and the data-analysis triangulation shows how the collected data were analysed for each case.

5.7 RESEARCH DESIGN OVERVIEW

This section will provide a brief overview of the research design and methodology that has been discussed thus far. Table 5.6 contains three columns. The first column notes the research aspect that is being discussed. Column two displays the options relating to the specific research aspect. Column three then displays the option that was selected in the context of this research study.

Table 5.6: Overview of the research design for the thesis

Research aspect	Alternatives	Selected alternative
HCI paradigm	• Traditional science • Design science • Engineering • Phenomenological matrix • Experience-centred design	Engineering
Research philosophy	• Positivism • Realism • Interpretivism • Objectivism • Subjectivism • Pragmatism • Functionalist • Interpretive • Radical humanist • Radical structuralist	Interpretivism
Research approach	• Deductive • Inductive	Inductive
Research strategy	• Experiment • Survey • Case study • Action research • Grounded theory • Ethnography • Archival research	Case study
Choices	• Mono method • Mixed method • Multi-method	Mixed methods
Time horizon	• Cross-sectional • Longitudinal	Longitudinal
Data collection techniques	Data collection and data analysis methods. Data triangulation will also be applied.	• Secondary data • Questionnaires • HE • FUE

In table 5.6, attention should be drawn to the fact that the six layers of the onion research model are discussed within the column headed “Research aspect”. However, it is also evident that two additional aspects are discussed in this column as well, which are not part of the research onion – the HCI paradigm and the Conceptual framework. Figure 5.9 illustrates the onion research model which has been adjusted for this particular research project. The HCI paradigm and conceptual framework aspects are not included in this figure. Therefore, figure 5.15 is provided to display the final research onion model to be applied. This onion incorporates the HCI paradigm and conceptual framework aspects as separate and additional layers to the existing model.

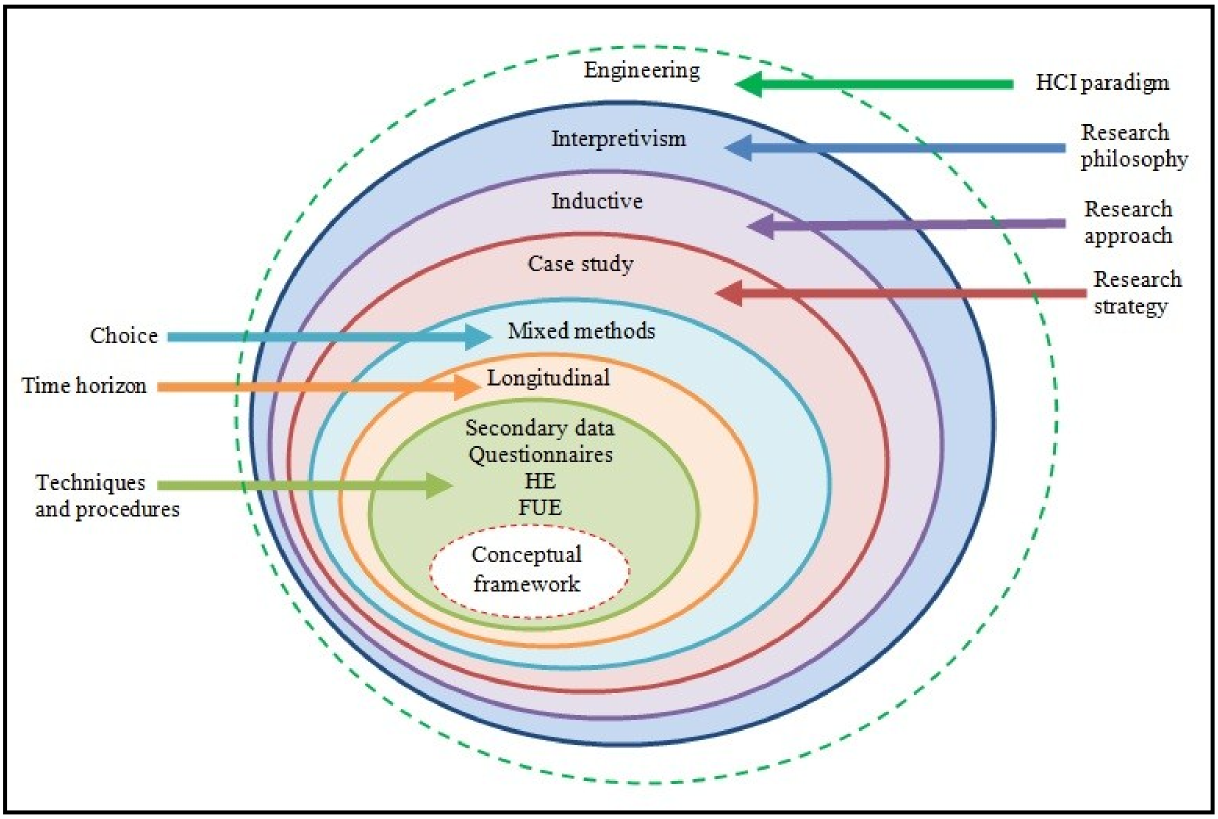


Figure 5.15: The improved research onion model to be applied for this study

It is practical for the researcher to first understand and know the paradigm in which the research will be undertaken. Once this has been done, focus can be directed towards the layers of the onion research model, starting with the philosophy and moving down to the actual techniques and procedures that will be used. It is for this reason that the HCI paradigm layer is situated at the exterior of the onion ring and before the Research philosophy layer. Figure 5.15 provides an indication of the research processes and considerations required in terms of the layers, in order to develop the USec framework. This is observed in terms of the ring representing the Conceptual framework, which is the goal and final ring that needs to be reached. However, this can only be achieved by accomplishing the requirements for all of the other layers that precede it.

A brief mention at this point to previous chapters that were discussed and chapters that are to follow is necessary. This will improve understanding regarding chapter flow, connection and progression in the thesis. To reiterate, chapter 1 presented the problem and discussed the research questions. In chapters 2 and 3 a theoretical investigation was conducted in HCI and USec respectively. Founded on secondary data (selected *data collection technique*) from these two chapters, a process to develop heuristics for SADs and a USec HE (first iteration) were established. Their development is presented and discussed in chapter 4. It must be noted that the USec HE (first iteration) is the outcome of completing phase 1 of the process. In chapter 5 the research design and methodology applied to this study is presented.

Chapter 6 discusses a multiple case study (selected *strategy*) that was conducted on two OHSNs. This includes the data collected and analysed from the participants using FUEs, HEs and user satisfaction questionnaires (selected *data collection techniques*). It must be noted that the case study is the outcome of completing phase 3 of the process. Chapter 7 discusses the results from the experts, whom evaluated the USec HE (first iteration) with the validation tool. The results are analysed and interpreted. It must be noted that the validation conducted is the outcome of completing phase 2 of the process. Following, chapter 8 presents the USec framework. It discusses the components and resulting relationships that have been formed based on chapters 4, 6 and 7. The components are the USec HE (second iteration), the process to develop heuristics for SADs and the validation tool. The conclusion of the thesis is presented in chapter 9.

5.8 ETHICS AND ANONYMITY

Ethical considerations are essential in research. The required ethical clearances were obtained by the university in order to conduct the research. The privacy and protection of the participants were also acknowledged. Trochim (2006b) discusses five key phrases to provide ethical protections in social and medical research. By considering these, the rights of the research participants will be fulfilled. These are discussed in the context of this research and include the following phrases:

1. *Voluntary participation*. People should not be forced to participate in the research. This usually occurs at universities or prisons where researchers will use "captive

audiences" as their subjects. The participants for the FUE were postgraduate students who participated voluntarily. The experts to conduct the validations were approached, and confirmed their participation or not.

2. *Informed consent.* This requires participants to be fully informed of the procedures and risks involved in the research. In addition they will need to provide their consent in order to participate. The participants in the FUE were provided with a consent form for each OHSN that they evaluated. This form stated the procedures of the research and required their signature to confirm their consent (see *Appendix B.43: Consent Form for MedHelp* and *B.44: Consent Form for Google Health*). No consent forms were required for the experts because they conducted their validations in their own time and space, using a validation tool that was created in this study to evaluate the USec HE, which is also an outcome of this study.

3. *Risk of harm.* Participants should not be placed in any situation in which they are at any risk of harm during the research. This includes physical and psychological harm. The FUE was conducted in a lab at the NMMU, which is the environment where the participants conduct their research work. Hence they were familiar with the surroundings and experienced no unease.

4. *Confidentiality.* This guarantees that identifying information of participants (if it exists) will only be available to people who are directly involved in the research. In this case, this includes the researcher and the supervisors of the study.

5. *Anonymity.* This guarantees that the participants remain anonymous during the course of the study. This is a stronger form of privacy than confidentiality; however, it is more difficult to accomplish. Anonymity will be assured by identifying participants with the letter "P" combined with a numeric value.

5.9 SUMMARY

This chapter focused on the research design and methodology of the study and is regarded as the most critical chapter of the research. There is a wealth of theory regarding research design and methodologies and, at times, the different theories may contradict one another, as to which method is better suited for a particular study and as to how it should be implemented. Therefore, the research design and methodology was discussed in detail by the use of a model. Moreover, the options selected at each level of the disintegration were supported in the context of this research study.

Before the model could be implemented, it was necessary to investigate the research paradigms that exist. These investigations led to the conclusion that the most suitable paradigm would be an engineering one. Once the paradigm was selected, it was then possible to introduce the model on which the research design and methodology would be based. This was the research onion model. In addition, the reasons for implementing the model were given. The model is divided into six layers: on layer one, the research philosophies were discussed – the chosen research philosophy was interpretivism. On layer two, the research approaches were discussed and inductive reasoning was chosen. The research strategies are the focus of layer three, where a case study is selected. On layer four research choices are considered. For this layer the mixed-model method was implemented. Time horizons are discussed on layer five and the option selected was a longitudinal study. The final layer, layer six, is dedicated to the research techniques and procedures. Combinations of options were employed that include secondary data, questionnaires, HE and FUE.

A discussion on frameworks then followed. It was important to understand the components and relationships involved in developing a framework, as such information is vital for developing the USec framework. Subsequently, the research questions for the study were mentioned. The study has one main research question that is supported by four sub questions.

Owing to the fact that a number of data collection techniques were used it is important to integrate the collected data, as improved data validity will result. This is achieved by means of data triangulation, which was the next section discussed. All of what had been discussed thus far in the chapter in terms of research design and methodology was then summarised in the next section, the research design overview. In accordance with the research design overview, figure 5.16 is presented. It recapitulates the research methodological process that was followed in this study to address the primary research question. The research methodological process is presented in two stages to distinguish between the preparation and the management of data. Stage 1 is concerned with the preparation, while stage 2 concentrates on data management. To conclude the chapter, the controls that would be put into place to ensure that ethical considerations are adhered to were mentioned.

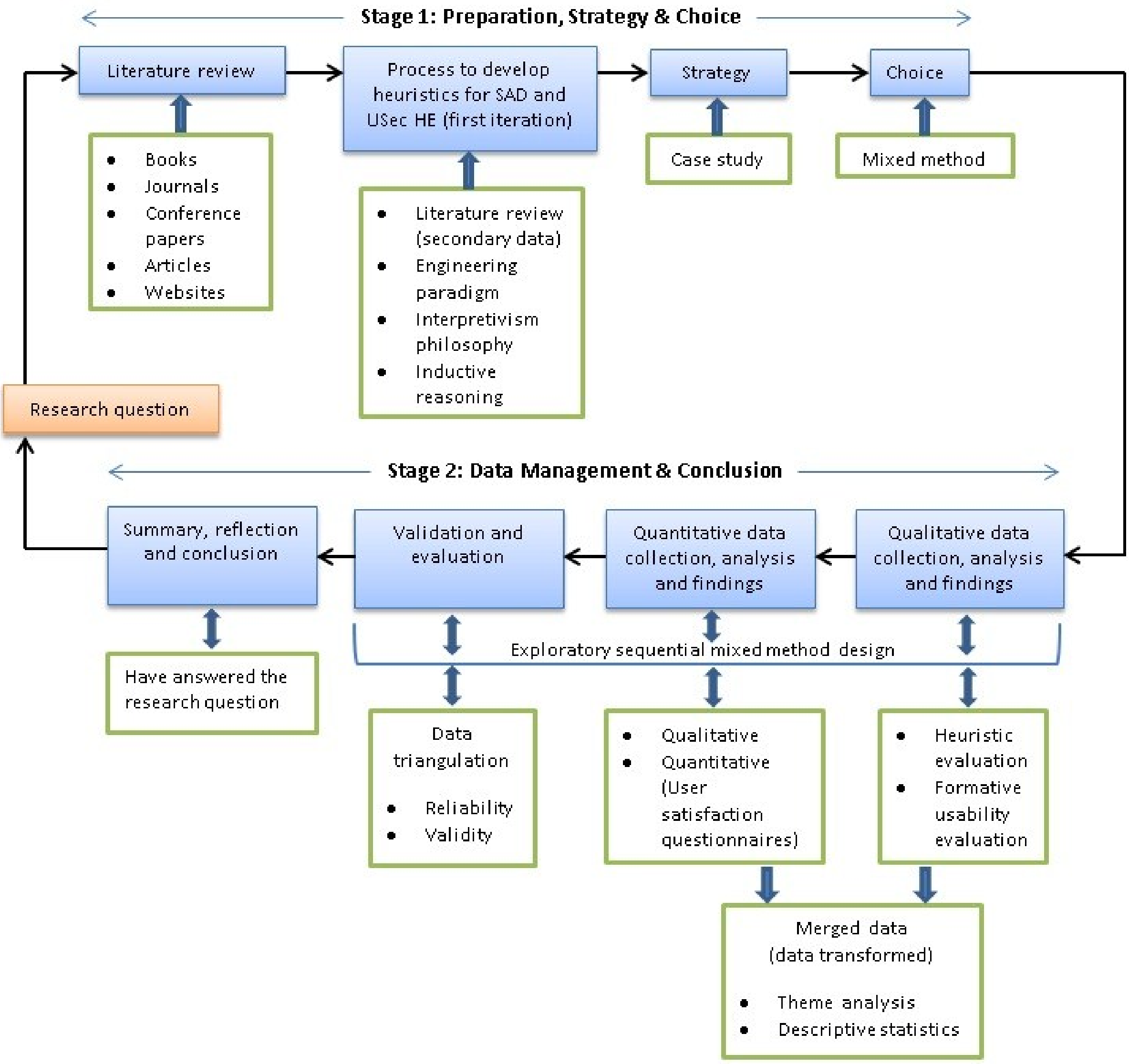
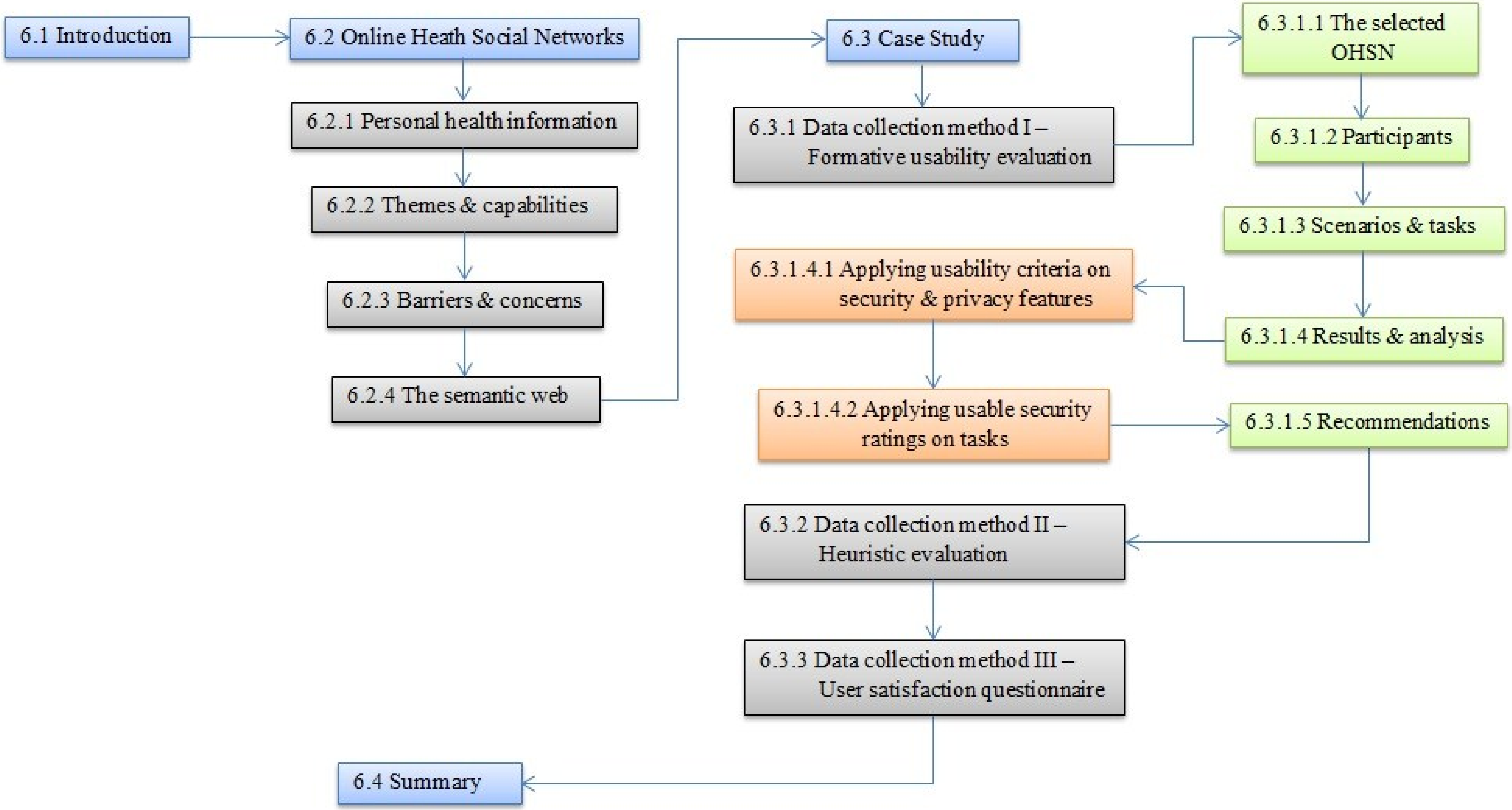

Stage 1: Preparation, Strategy & Choice
Literature review
Process to develop heuristics for SAD and USec HE (first iteration)
Strategy
Choice
Books
Journals
Conference papers
Articles
Websites
Literature review (secondary data)
Engineering paradigm
Interpretivism philosophy
Inductive reasoning
Case study
Mixed method
Research question
Stage 2: Data Management & Conclusion
Summary, reflection and conclusion
Validation and evaluation
Quantitative data collection, analysis and findings
Qualitative data collection, analysis and findings
Exploratory sequential mixed method design
Have answered the research question
Data triangulation
Reliability
Validity
Qualitative
Quantitative (User satisfaction questionnaires)
Heuristic evaluation
Formative usability evaluation
Merged data (data transformed)
Theme analysis
Descriptive statistics

Figure 5.16: The research methodological process

LAYOUT OF CHAPTER 6


6.1 Introduction
6.2 Online Heath Social Networks
6.2.1 Personal health information
6.2.2 Themes & capabilities
6.2.3 Barriers & concerns
6.2.4 The semantic web
6.3 Case Study
6.3.1 Data collection method I – Formative usability evaluation
6.3.1.1 The selected OHSN
6.3.1.2 Participants
6.3.1.3 Scenarios & tasks
6.3.1.4 Results & analysis
6.3.1.4.1 Applying usability criteria on security & privacy features
6.3.1.4.2 Applying usable security ratings on tasks
6.3.1.5 Recommendations
6.3.2 Data collection method II – Heuristic evaluation
6.3.3 Data collection method III – User satisfaction questionnaire
6.4 Summary

CHAPTER 6: CASE STUDY – ONLINE HEALTH SOCIAL NETWORKS

6.1 INTRODUCTION

This chapter will discuss the case study conducted on OHSNs. This case study applied three data collection methods: an FUE, a HE and a user satisfaction questionnaire.

Section 6.2 will introduce OHSNs and related information. Section 6.3 presents the results from the case study and, based on the analysis, recommendations and conclusions are made. A summary is presented in section 6.4.

6.2 ONLINE HEALTH SOCIAL NETWORKS

Social networking describes a host of interactions between individuals within a social network. Online social networking tools exploit Internet technologies to support social networking actions among people. These tools may assist health organisations to better understand the needs of their consumers who use health and social care services, as they provide the people with a "voice" to help improve health services along all boundaries and to promote an increased health conscious (Purdy, 2008).

A critical factor for the adoption of health social networking tools is that they are easy to use. People should be able generate and share health content easily. Some of the more popular tools include wikis, blogs, podcasting/vodcasting, social bookmarking, collaborative tagging (or folksonomies), tag clouds, instant messaging, email, mashups, and RSS feeds. These tools form part of Web 2.0, the current evolution of the Internet. Some of the tools are discussed in table 6.1. Popular websites where the particular tools are being used are also provided. In addition, examples relating to the health field are provided (Boulos & Wheelert, 2007; Purdy, 2008).

Table 6.1: Web 2.0 tools

Web 2.0 tool	Common examples (not in health field)	Examples in health field
Wikis: collaborative software tools that permit users to add content, yet that content can be subject to editing by any person.	Wikipedia: http://www.wikipedia.org/	Wiki Surgery: http://www.wikisurgery.com Flu Wiki: http://fluwikie.com
Blogs: simple content	Most social networking	DrugScope DrugData Updated blog:

Web 2.0 tool	Common examples (not in health field)	Examples in health field
management tools. They provide non-experts with the ability to build Web diaries or online journals.	websites provide blog features	http://drugscope.wordpress.com/ Lord Darzi's Blog: www.ournhs.nhs.uk/category/darzi/
Podcasting /vodcasting: permits digital downloads in audio and video formats from websites to MP3 and MP4 players.	YouTube: http://www.youtube.com/	New England Journal of Medicine podcasts Johns Hopkins Medicine podcasts
RSS feeds: permit users to automatically be notified of new content and updates on websites of their interest.	CNN: http://edition.cnn.com/services/rss/	BBC News Health: http://newsrss.bbc.co.uk/rss/newsline_uk_edition/health/rss.xml New Scientist – Health: http://pheedo.com/f/newscientist_health/rss10
Mashups: provide capabilities for integration and derivative work by combining two or more pieces of digital media from different sources.	Digg: http://www.digg.com/	HealthMap: http://www.healthmap.org

The fact that Web 2.0 social networking tools are being used within the health and medical fields has led to the development of various social health systems terminologies. New terminologies have surfaced, including eHealth, PHR 2.0, Health 2.0, patient portals and Medicine 2.0 (Hughes et al., 2008). These systems are mostly integrated with Web 2.0 tools (as implied from the "2.0" extension in their terminologies). In this study these types of website are termed *OHSNs*. There is ample space for innovation in this area. For example, industry is currently investigating solutions that can offer users more useful information, collected from their physical activity monitoring devices (Yeratziotis, Sannemann, Viitanen & Nieminen, 2011). This can provide a platform for service integration with OHSNs and other services.

6.2.1 Personal Health Information

ISO 27799 (Health informatics – Information security management in health using ISO/IEC 27002) defines personal health information (PHI) as "information about an identifiable person which relates to the physical or mental health of the individual or to provision of health services to the individual" (ISO/IEC 27799, 2008). This includes the following (ISO/IEC 27799, 2008):

- Registration information of the individual required for the provision of health services.
- Payment information or eligibility for health care with regard to the individual.
- Information to uniquely identify the individual for health purposes (e.g. number or symbol).
- Information about the individual collected in the course of the provision of health services.
- Information derived from testing or examinations of a body part or bodily substance.
- Identification of a person (e.g. a health professional) that provides healthcare to the individual.

Support for patient control over PHI is now more evident than ever before (Halamka, Mandl & Tang, 2007). This is considered to be an appealing approach, given that it solves the consent and privacy issues that organisations face in the exchange of health data. The emphasis is on providing patients with custody over the PHI. They can therefore utilise their PHI in various ways. When patients are empowered and provided with such custody, they become personally responsible for protecting the confidentiality of their information. The outcome is accelerated health information exchange, as consent is no longer considered a barrier (Halamka et al., 2007).

Patient control of health data may indeed be a desirable prospect. However, this has to be done in a methodical manner. The answer is not to remove security responsibilities from health care organisations and transfer them over to the patients, without assisting them in security matters. In order to succeed, issues such as privacy, policies, data ownership and personal control need to be investigated (Halamka et al., 2007). These security issues need attention from two perspectives: the health-care providers' side and the patients' side. This case study is concerned with the security and privacy aspects commencing from the patient perspective in OHSNs.

6.2.2 Themes and Capabilities

An in-depth analysis of Health 2.0 and Medicine 2.0 assists in identifying similarities in a number of key and prominent themes. These themes are representative of online social networking environments and most, if not all, should be integrated in other health social systems as well. The themes include the following (Hughes et al., 2008; Eysenbach, 2008):

1. Participation – The participants that are involved (e.g. doctors, patients, nurses). This empowers end-user participation and has resulted in a health care culture change.
2. Collaboration – The impact on traditional and collaborative practices in medicine.
3. The ability to provide health care which is personalised.
4. The promotion of ongoing medical education.
5. The associated method- and tool-related issues (e.g. the potential for inaccurate content provided by the end-user).
6. Social networking – It is central to Web 2.0 applications and provides the basis for people to create connections.
7. Apomediation – This relates to users identifying trustworthy and credible information and services over the Web 2.0.
8. Openness – This relates to Web 2.0 from standards, transparency, interoperability, open source, and open interfaces' perspectives. This also includes transparency and openness to information that was previously of limited access.

Web 2.0 communities compile a wealth of information on selected topics for shared knowledge rather than for individual knowledge. This information centres on social networking and has revolutionised the manner in which people collaborate and communicate. By creating an online community for patients, a Web 2.0 community may be developed that promotes conversations regarding health practices (Frost & Massagli, 2008; Eysenbach 2008).

An important aspect of OHSNs is that they are not only fun, like Facebook or Flicker, but that they also need to be secure and trustworthy. They also need to provide immediate benefits for the users, as well as incentives (Yeratziotis et al., 2011). This will motivate users to participate and contribute constructively in a health virtual community (Eysenbach, 2008). These websites are mainly designed for the patient population and their success depends on the utilisation of PHI by its users. Hence, security and privacy is critical.

OHSNs provide patients with the capabilities to interact and communicate with their healthcare providers. Some of the more popular websites include MS HealthVault, Google Health, Care Converge, MedHelp, MEDSEEK, and PatientsLikeMe. There is optimism regarding the advancement and adoption of OHSNs in the future (Kuhn, 2008; Eysenbach, 2008).

OHSNs benefit healthcare providers and patients equally because they increase productivity and efficiency. Depending on their level of functionality, patients are able to register and complete forms online. This saves time and reduces physical visits to healthcare providers. Patients can request prescription refills online, make medication requests and order health equipment (e.g. glasses, contact lenses). They can also access medical records and health information and receive their lab tests and x-rays. In addition, they can pay bills and schedule appointments.

Patients are able to communicate directly with their healthcare providers (e.g. ask questions and/or leave comments) in simply-tracked, well-managed, documented and evaluated methods (Katz & Moyer, 2004; Alder, 2006). OHSNs may be free-standing or integrated with a system owned by the health care provider. In essence, these technologies can help revitalise primary care, improve patient–doctor communication and enhance patient access (Alder, 2006). To summarise, the key benefits of OHSNs are the following (Katz & Moyer, 2004):

1. They address patient communication with the health care providers. This is a need that was not met before. As a result, patient satisfaction will improve and service delivery will be more effective.
2. Efficiency of service delivery will be improved even more by substituting non-efficient communication styles with more efficient ones (e.g. through improved management of medical problems).
3. Business practices are improved because patient billing and registration becomes more efficient.

Research proves that by providing patients with their online health records, communication and trust with their healthcare providers improves (Frost & Massagli, 2008). The patient data are also better completed and the overall clinical encounter is one of better quality. However, providing patients with static medical information can be overwhelming. If patients are to interpret this information correctly, the health record must be more than just a static repository of health data. It should rather support patients in combining different sources of data, and provide knowledge as well as software tools in which patients may become active participants in their own health (Frost & Massagli, 2008).

6.2.3 Barriers and Concerns

The benefits of OHSNs are evident; however, there are many barriers that will need to be overcome for successful implementation. Already mentioned are aspects such as the compensation for services, patient privacy and confidentiality, practical workflow concerns and medico-legal concerns (Alder, 2006). In addition, the overwhelming numbers of online messages from the patients must be managed; websites need to be easy to use; assurance should be given that the interpersonal relationships between physicians and patients will not be lost; and patients educated about privacy concerns (Zickmund, Hess, Bryce, McTigue, Olshansky, Fitzgerald, et al., 2007). These issues relate to privacy, security, usability and UX. Therefore, the concept of USec is critical in such an environment.

The potential of well-designed OHSNs is clearly understood. However, these systems will only fulfil their potential if the patients themselves know how to use them effectively. To achieve this, the websites must be user-friendly and meet the particular needs of the patients. This will ensure that they are helpful and also accepted by the patients. This requires OHSNs to be evaluated according to usability, satisfaction and helpfulness criteria derived from the patients' perspective. They will also need to effectively promote health information (Farzanfar, Finkelstein & Friedman, 2004).

6.2.4 The Semantic Web

The Internet is currently in the Web 2.0 era, which makes use of social networking tools that facilitate collaboration, sharing and openness of information and resources. The next level of the Web is referred to as Web 3.0 or the *semantic Web*. There have been a wide range of definitions to explain this term, which have caused debate. A definition provided by John Markoff defines *Web 3.0* as "a set of technologies that offer efficient new ways to help computers organize and draw conclusions from online data" (Borland, 2007).

The purpose of Web 3.0 is to make computers understand information without human intervention. This will enable them to do most of the work relating to the finding and sharing of required information (Mortimer, 2007; Borland, 2007). The *semantic Web* and *Web 3.0* are terms that are used interchangeably. One may argue that the term *Web 3.0* is used as a marketing ploy more than anything else. The term, *semantic Web,* is used because the primary feature of this version of the Web is to use metadata. It also requires the use of semantic annotation within Web documents in order to articulate meaning, as expressed by Berners-Lee (in Giustini, 2007). This would entail blending semantic Web data-handling techniques with Web 2.0 features (Borland, 2007). The use of software and intelligent agents is critical for its success (Metz, 2007; Mortimer, 2007), as these agents will make decisions on behalf of the user (Mortimer, 2007). In some cases, it has been said that the "thing" called Web 3.0 is only a subset of the semantic Web vision (Borland, 2007).

The semantic Web is at a vastly theoretical stage and will take time to fulfil its promise (Hughes et al., 2008; Eysenbach, 2008). If it does fulfil it, the Web will become easier to use. Computers will perform tasks on the users' behalf so that they may focus on their work (Giustini, 2007). However, some businesses have already started to adopt the new technologies. They are applying the simpler semantic Web tools at the moment while avoiding the more ambitious ones. Tools such as providing once-inaccessible data sources online, improving automate database searches, helping users select holiday destinations and sorting through complicated financial data more efficiently are already being implemented (Borland, 2007).

For the health industry, Web 3.0 is deemed to be a necessary component for better health practices. In fact, the medical industry is one of the first groups involved in the development of the semantic Web. The W3C (World Wide Consortium) has thus launched the Health Care and Life Sciences Interest Group. They are chartered to "develop and support the use of semantic Web technologies and practices to improve collaboration, research and development, and innovation adoption in the Health Care and Life Science domains. Success in these domains depends on a foundation of semantically rich system, process and information interoperability" (Jessen, 2007).

Doctors will be able to find the information they require instead of just searching for it, as they do in the "unorganised" Web 2.0. Medical librarians also believe it will lead to the development of better mechanisms for information retrieval, as this is becoming increasingly difficult at the moment (Giustini, 2007). Bioinformatics and systems biology in particular will benefit from using Web 3.0 and data representation and management will improve considerably. The processing of large quantities of data, in disparate systems with rich semantic tools will provide knowledge discovery (Jessen, 2007). Giustini, (2007) believes that publishing clinical data that can be scrutinised openly will also produce a wealth of medical knowledge.

Another outcome from Web 3.0 is the development of a personalised healthcare system or personalised medicine, as it is better referred to. The tools will be in place to analyse genetic profiles, once again due to the quantities of information being produced. This will assist in treating patients' health problems according to their own personal information gathered. However, providing patients with better ways to manage their disease based on their genetic and environmental profile will be a challenge (Jessen, 2007). But the huge datasets and virtual three-dimensional tools may help provide treatments for new diseases and natural disasters (Giustini, 2007).

Modern health care applications for both patient and health-care provider use are generally embedded with social tools and capabilities in their design. A contradiction tends to surface here, as these tools promote free sharing of personal information over the Internet, yet security of PHI remains a key priority and in many cases an obstacle to the adoption of these tools. Improved designs are required to ensure that users can share and use PHI and be guaranteed that it is done in the most secure and trustworthy manner. This approach must also be easy to understand and use for the end-users.

Part of the solution to this is to apply USec practices to the design of an OHSN. The research conducted in the areas of USec and InfoSec needs to be combined and addressed in an understandable context. This context will provide input into the development of a framework for USec in online social networking environments; a framework that is equally imperative for both users and developers. The main outcome will be a comprehensive and theoretical guide for the developers, which will provide them with the ability to enhance their services to end-users. This will be achieved by ensuring security and usability is a unified process, which can be incorporated into the design of their software. As a result, user competencies and preferences will be acknowledged, leading to USec.

6.3 THE CASE STUDY

A multiple-case study (Yin, 2008) was conducted on two OHSNs. This strategy examines various cases. Such studies can offer a complete representation of UX's interaction with products; evaluating its effectiveness via its strengths and weaknesses. This provides a range of constructive information for analysis, from which data patterns emerge, improving thereby the product, once recommended changes have been implemented. The data collection techniques within the case study consisted of an FUE, a HE and a user satisfaction questionnaire. The case study will be discussed in this section.

6.3.1 Data Collection Method I – Formative Usability Evaluation

A FUE, as discussed in section 5.5.8.3, was conducted as part of the case study. The FUE method is used by development teams to evaluate a product. Accordingly, one needs to know what information can be obtained by the evaluation beforehand (Benyon et al., 2005). This method was used to assess the USec on the two websites. The purpose of the FUE method as applied in the broader research study is twofold:

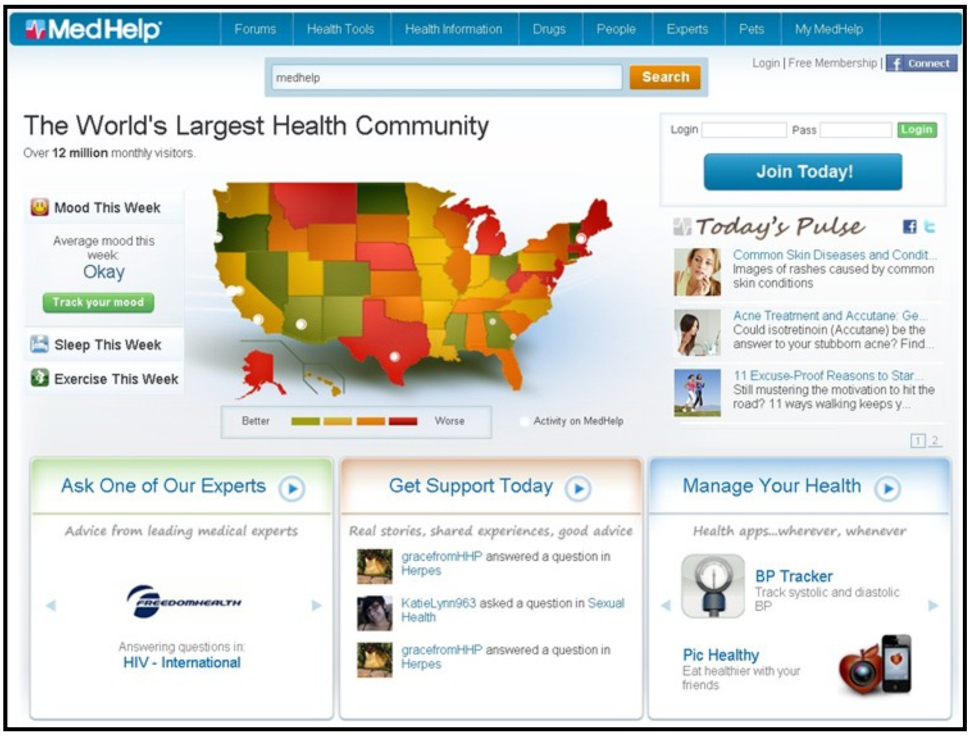
1. Test the application of the new USec HE that was developed and reported in chapter 4 (Yeratziotis et al., 2012). The USec HE is a tool for determining security and privacy usability violations on interfaces.
2. Assess the level of USec on the two websites (Yeratziotis, Pottas & van Greunen, 2011b). Therefore, it is necessary to determine how usable the security/privacy features and information are that participants need to interact with and understand. This would be a comparative study that would help determine the "do's and don'ts" with regard to the design of security and privacy on an OHSN. As a result, recommendations can be provided for improving USec on OHSNs.

6.3.1.1 The Selected OHSNs

The FUE was conducted on two OHSNs. These were Google Health and MedHelp. Figure 6.1 presents the MedHelp homepage and figure 6.2 presents the webpage that users are directed to once they have logged-in to Google Health. As mentioned in section 5.5.8.3, a selection procedure was followed to determine the OHSN to be studied. The selection procedure is summarised as follows:

1. Review literature in online social networking and OHSNs to identify characteristics.
2. Develop and apply the requirements based on the characteristics identified previously. This resulted in 21 candidate websites.
3. Develop and apply a minimum set of requirements on the 21 websites, resulting in seven candidate websites.
4. Apply bonus requirements to the seven websites to determine the final 2 websites for the study.

MedHelp is an online health community that connects people with medical experts and others who have similar experiences. It empowers over 12 million people each month to take control of their health. It is a privately-funded company that has long-standing partnerships with the top medical institutions. The infrastructure allows patients actively to manage their health through its condition-specific health applications and Personal Health Records (PHRs).



The World's Largest Health Community

Over 12 million monthly visitors.

Mood This Week

Average mood this week: Okay

Track your mood

Sleep This Week

Exercise This Week

Today's Pulse

Common Skin Diseases and Condit... Images of rashes caused by common skin conditions

Acne Treatment and Accutane: Ge... Could isotretinoin (Accutane) be the answer to your stubborn acne? Find...

11 Excuse-Proof Reasons to Star... Still mustering the motivation to hit the road? 11 ways walking keeps y...

Ask One of Our Experts

Advice from leading medical experts

FREEDOMHEALTH

Answering questions in: HIV - International

Get Support Today

Real stories, shared experiences, good advice

gracefromHHP answered a question in Herpes

KatieLynn963 asked a question in Sexual Health

gracefromHHP answered a question in Herpes

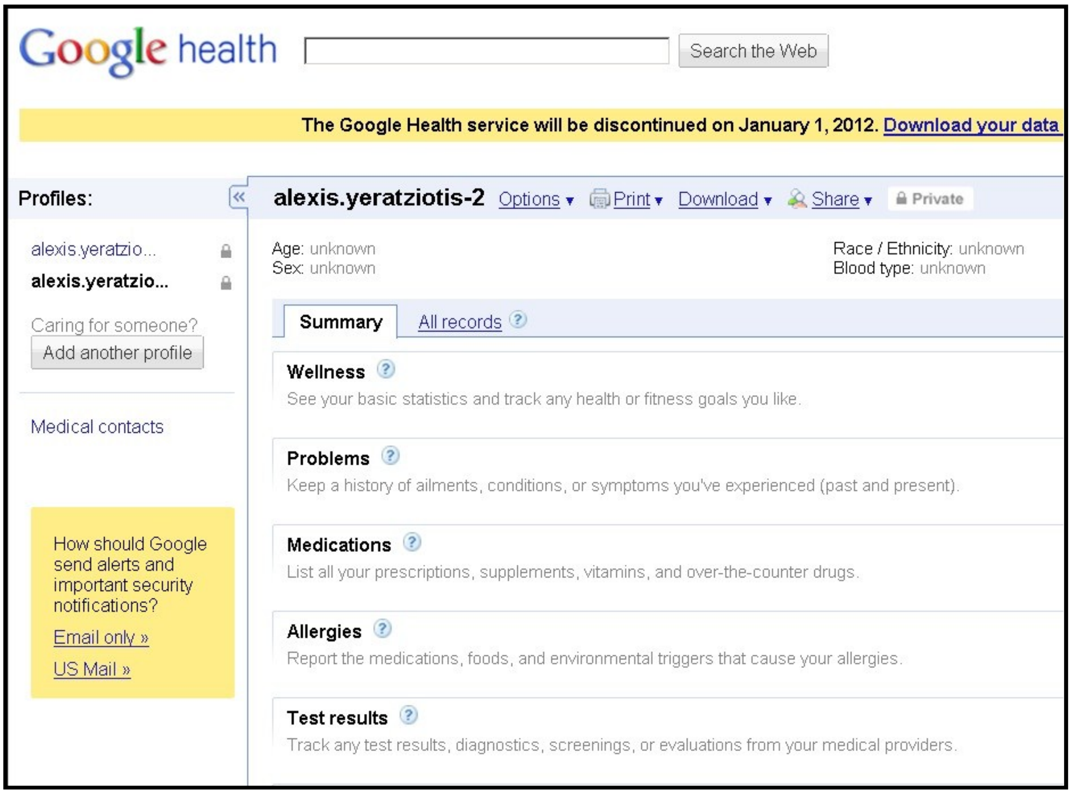
Manage Your Health

Health apps...wherever, whenever

BP Tracker
Track systolic and diastolic BP

Pic Healthy
Eat healthier with your friends

Figure 6.1: MedHelp homepage (http://www.medhelp.org/)



The Google Health service will be discontinued on January 1, 2012. Download your data

Profiles:

alexis.yeratzio...

alexis.yeratzio...

Caring for someone?

Add another profile

Medical contacts

How should Google send alerts and important security notifications?

Email only »

US Mail »

alexis.yeratziotis-2

Age: unknown
Sex: unknown

Race / Ethnicity: unknown
Blood type: unknown

Wellness
See your basic statistics and track any health or fitness goals you like.

Problems
Keep a history of ailments, conditions, or symptoms you've experienced (past and present).

Medications
List all your prescriptions, supplements, vitamins, and over-the-counter drugs.

Allergies
Report the medications, foods, and environmental triggers that cause your allergies.

Test results
Track any test results, diagnostics, screenings, or evaluations from your medical providers.

Figure 6.2: Google Health webpage once logged-in (www.google.com/health/)

Google Health allows users to organise, track, monitor, and act on their health information. With a Google Health account, users can store, manage and share all their health and wellness information in one central place. It allows users to share their information with whomever they want. Google Health uses sophisticated security techniques to help keep users' information secure and private.

This study has been examining Google Health since 2009, but, it should be noted that Google retired the Google Health service on 1 January 2012. (http://googleblog.blogspot.com/2011/06/update-on-google-health-and-google.html).

Users will be able to download their data in various formats until 1 January 2013. The reason for this is that Google Health was designed to provide people with access to their personal health information in a consumer-centred approach. Accordingly, Google wanted to have an impact on the day-to-day health experiences of millions of users. After a few years of existence, however, it has not had the desired effect and has only been adopted by certain user groups (e.g. tech-savvy patients and their caregivers, fitness and wellness enthusiasts). In essence, Google has not been successful in translating the limited usage into widespread adoption in the daily health routines of millions of people.

6.3.1.2 Participants

A total of six participants were used in the usability evaluations. The participants were postgraduate students from the field of ICT. Table 6.2 provides more detail about the participant profiles.

Table 6.2: Participant profiles

Participant	**Level of studies**	**Research focus**
P1	PhD	Health informatics
P2	Masters	Health informatics
P3	Masters	InfoSec
P4	Masters	InfoSec
P5	PhD	HCI
P6	PhD	HCI

The participants can be considered as computer experts, which may have affected their perceptions and judgments. However, supporting their selection is the fact that they had a familiarity with social networks (e.g. Facebook), allowing them to express informed opinions. It would have been preferred to have participants with experience on OHSNs specifically, but it was difficult to identify such participants, as OHSNs are a relatively unknown online service in South Africa and most are limited to users in America and Europe. Another difficulty with recruiting such participants would have been their reluctance to share their "real" health information with a researcher. In the light of these constraints, it is believed that the postgraduate students provided a viable and sensible selection of participants.

6.3.1.3 Scenarios and Tasks

Once the OHSNs were selected, participants were provided with scenarios. These are stories that provide general descriptions about the surrounding context. This helps participants to better understand the user that they are representing as a potential user of the website. The tasks are more specific and describe the actions that a participant will need to perform during the usability evaluation. These were typical tasks that users of an OHSN would need to perform in a real-life context. The tasks in the scenarios addressed interactions of a security/privacy nature.

An initial scenario was provided for each OHSN. Based on this scenario, a total of seven tasks needed to be conducted on the MedHelp and Google Health websites. Each of the seven tasks included their own sub-scenarios that built on the initial scenario. Additionally, in order to achieve the goal of a task, a number of sub-tasks would need to be completed. The participants also had the option to provide comments for each sub-task, including both negative and positive comments. The tasks are described in table 6.3. The numbers in brackets next to the task represent the number of subtasks that need to be performed to complete the overall task in MedHelp and Google Health respectively.

Table 6.3: The tasks for the FUE

Task	Description	Purpose
1	Home page impression (8) (8)	To determine if the participants' impression of the homepage instils trust and how it impacts on their decision to register on the website.
2	Registration process (17) (17)	In order to use the full capabilities of the website, users' are required to register and create an online user profile. Participants' created a user profile with minimum personal

		information.
3	Account settings/My account (23) (18)	Users' may be concerned about protecting their personal information as well as possible. A central place where they can configure all the security and privacy settings for their user profile is required. This central place is referred to as "Account settings" in MedHelp and "My account" in Google Health.
4	Find a friend/Share your profile (5) (9)	This task examined the process of sharing information with other patients. In MedHelp the participants were required to send a friend invitation before sharing information. Google Health does not allow for the concept of creating friends. However, it allows users to share their profile with others by sending a share request.
5	Find a doctor/Import your medical record (8) (10)	The participants were required to find a doctor on MedHelp and assess the profile of that doctor. In Google Health, they would need to have an online medical record to share information and communicate with health-care providers. Participants' examined the process of doing both without making real communication with health-care providers or importing medical records in both MedHelp and Google Health.
6	Website online policies (11) (10)	This task focused on the website policies. Policies are provided to users during registration, yet it is debatable whether these will be perused in detail at this stage.
7	Security considerations (6) (7)	This task mentioned several security considerations regarding the websites. It did not require participants' to complete any tasks. They just had to provide their comments (if any). These considerations included identity signals (certificates), session locks, simultaneous connections to a profile, deleting a profile and third-party websites.

The case study evaluated the security and privacy features of the two OHSNs. It is important to clarify that the usability criteria applied are measuring the security and the privacy features of the websites alone and not the overall usability of the websites. The results presented are based on evaluating the security and privacy features in terms of usability criteria and on evaluating the task in terms of USec.

6.3.1.4 Results and Analysis

The results from the FUE are now presented. Following the analysis, recommendations are made for improving the level of USec on both OHSNs.

6.3.1.4.1 Applying usability criteria on security and privacy features

The specific usability criteria include ease-of-use, terminology, ease-of-learning, feedback, awareness, errors, and help and documentation. In addition to these, trust, which is not necessarily a usability criterion, is also measured. Trust has an impact on UX and in order to use OHSNs to their full capabilities, they need to provide security and privacy features that can gain user trust. The selected usability criteria measure the following aspects:

- *Ease-of-use* - Measures the security/privacy features on the basis of characteristics such as simplicity, user-friendliness, flexibility and least steps in completing a task.
- *Terminology* - Measures the logical, natural order of information. It uses phrases and concepts familiar to users and avoids complicated security/privacy terms. This is commonly known as speaking the users' language.
- *Ease-of-learning* - Measures the ease in learning to use the security/privacy features, as well as ease in remembering features after not using them for a time. Ease of learning allows users to build on their knowledge without deliberate efforts.
- *Feedback* - Measures timely feedback in response to participants' security actions. It is important that users are always informed about the status of their actions.
- *Awareness* - Consequences must be made apparent to users before performing the actual security actions. Users must also be aware of their own security status.
- *Errors* - Measure the level of protection that users have to avoid making security errors. If errors occur, the problem and its solution must be provided. Messages must be in plain language so that users can recover from the error.
- *Help and documentation* - Measures the level of guidance and assistance users need to complete security tasks. A usable website minimises the need for assistance. However, it is practice to provide help and documentation in case these are required. Similar to providing help for general tasks, which are the users' primary goals, support for security information and instructions, which are generally the users' secondary goals, is also necessary.
- *Trust* - Measures the participants' confidence in correctly performing security tasks and providing personal information.

Usability criteria were represented in several sub-tasks. After evaluation, participants provided an overall rating based on acknowledged usability criteria (Pierotti, 1995; Nielsen, 2006). Tables 6.4 and 6.5 represent the frequency of the participants' responses (n = 6). The scores are representative of the number of users that selected the following: VG = Very Good; G = Good; BA = Barely Acceptable; P = Poor; and VP = Very Poor. The total for the responses are accumulated for each score as well. The intention is to identify usability criteria that are lacking in some way, and to improve these to a level of *Good*. Achieving an average of *Very Good* is the ultimate objective; thereby, achieving the best UX for patients interacting with the website's security and privacy features.

Table 6.4: Overall usability ratings for security and privacy features on MedHelp

Usability criteria	**VG**	**G**	**BA**	**P**	**VP**
Trust	1	2	1		2
Ease-of-use	2	3	1		
Terminology		4	1	1	
Ease-of-learning	1	3	2		
Feedback		3	1	2	
Awareness	1	3		2	
Errors		1	4	1	
Help & documentation	1	2	1	2	
TOTAL	6	21	11	8	2

Table 6.5: Overall usability ratings for security and privacy features on Google Health

Usability criteria	**VG**	**G**	**BA**	**P**	**VP**
Trust	2	4			
Ease-of-use	2	4			
Terminology	4	2			
Ease-of-learning	1	5			
Feedback		5	1		
Awareness	1	5			
Errors		2	2	2	
Help & documentation	1	5			
TOTAL	11	32	3	2	

A total of six participants evaluated the security and privacy features of MedHelp and Google Health according to eight usability criteria. This provided a total of forty-eight participant responses for each OHSN. The responses from each OHSN are compared in the graph in figure 6.3. The graph indicates that Google Health's security and privacy features are more usable than those of MedHelp. Following figure 6.3 is a detailed discussion on the usability criteria and their relating scores for each OHSN.

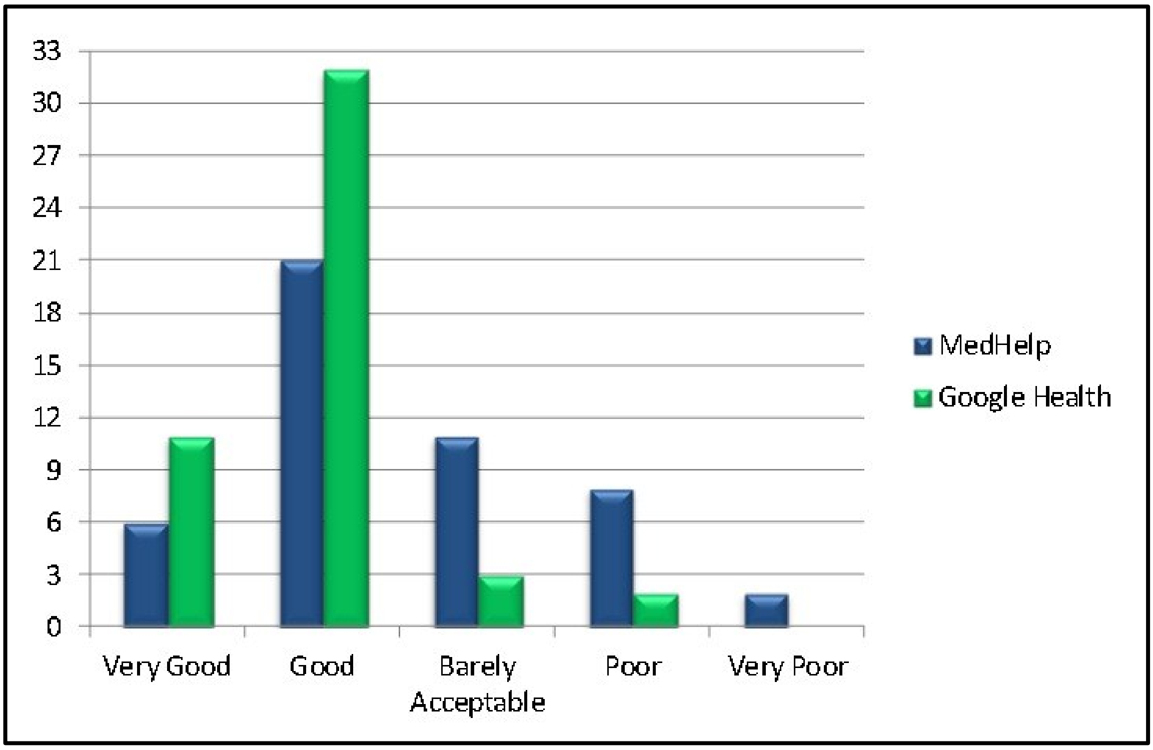


Figure 6.3: Comparison on the usability of MedHelp and Google Health's security and privacy features

With regards to the *Trust* criterion, Google Health scored higher than MedHelp. Participants' with a *Very Good* or *Good* trust relationship on Google Health occurred less often on MedHelp. What is alarming is the *Barely Acceptable* and *Very Poor* trust relationships built between participants' and MedHelp.

With regards to the *Ease-of-use* criterion, Google Health scored marginally better than MedHelp. Overall, ease-of-use was *Very Good* or *Good*. However, one participant rated MedHelp as *Barely Acceptable*.

With regards to the *Terminology* criterion, Google Health scored higher than MedHelp, with *Very Good* and *Good*, while MedHelp scored a *Good* rating overall. However, *Barely Acceptable* and *Poor* ratings also occurred.

With regards to the *Ease-of-learning* criterion, Google Health scored higher than MedHelp with *Very Good* and *Good*, while MedHelp averaged a *Good* score with one *Very Good* and two *Barely Acceptable* scores.

With regards to the *Feedback* criterion, Google Health scored higher than MedHelp, with *Good* for all participants except one, who deemed it *Barely Acceptable*. MedHelp had three *Good* scores, one *Barely Acceptable* and two *Poor* scores.

With regards to the *Awareness* criterion, Google Health scored higher than MedHelp on this measure, with an average *Good*, which included one *Very Good* score. MedHelp barely averaged a *Good*, with one *Very Good* score. However, it included two *Poor* scores, which are concerns.

With regards to the *Errors* criterion, both websites scored low and averaged *Barely Acceptable*.

With regards to the *Help and documentation* criterion, Google Health scored higher than MedHelp with an average *Good*, with one *Very Good* score. MedHelp had mixed scores, with one *Very Good*, two *Good*, one *Barely Acceptable* and two *Poor* scores. The inconsistency of the scores, the *Barely Acceptable* and *Poor* scores were a concern.

The results indicate that Google Health has higher levels of usability with regard to its security and privacy features. Terminology scored a *Very Good*, while other usability criteria, apart from errors, averaged *Good*, thereby being acceptable, even though they could be improved. The only real concern was with the errors criterion; this averaged *Barely Acceptable* and requires improvement. Following this, of lesser concern, is the feedback criterion.

MedHelp requires substantial improvements on many usability criteria. The ease-of-use, terminology and ease-of-learning criteria are acceptable, although these could be considerably improved. Immediate attention and improvements is needed for trust, feedback, errors, help and documentation.

6.3.1.4.2 Applying usable security ratings on tasks

Participants provided their overall ratings for the seven tasks, based on their UX in performing the tasks. They had to measure the two criteria defining USec in performing the overall task and its subtasks – how usable and secure those features were. Tables 6.6 and 6.7 represent the frequency of the participants' responses (n = 6). The scores are representative of the number of participants' that selected the following: S & U = Secure & Usable; S & MU = Secure & Moderately Usable; S & NU = Secure & Not Usable; NS & U = Not Secure & Usable; and NS & NU = Not Secure & Not Usable. A total for the responses is accumulated for each score as well. In table 6.6, note that there are five answers instead of six for Task 1. This was because one participant provided no rating here.

Comparisons were based on how usable and secure the tasks were for the participants, according to their experiences. The goal is to identify the tasks that are weak from a USec perspective: either from a lack of security, usability, or both. Once identified, improvements can be made in performing a task, resulting in a more secure and usable experience for the users. Tables 6.6 and 6.7 represent the frequencies of the participants' responses (n = 6).

Table 6.6: Overall security and usability ratings for the tasks on MedHelp

Task	S & U	S & MU	S & NU	NS & U	NS & NU
1 – Home page impression	2	1			2
2 – Registration process	3	1	1	1	
3 – Account settings/My account	2	2			2
4 – Find a friend/Share your profile	2	1	2	1	
5 – Find a doctor/import your medical record	1	3		1	1
6 – Website online policies	2	2		2	
7– Security considerations	1	2		1	2
TOTAL	13	12	3	6	7

Table 6.7: Overall security and usability ratings for the tasks on Google Health

Task	S & U	S & MU	S & NU	NS & U	NS & NU
1 – Home page impression	4	2			
2 – Registration process	5	1			
3 – Account settings/My account	2	4			
4 – Find a friend/Share your profile	5	1			
5 – Find a doctor/import your medical record	2	3		1	
6 – Website online policies	4	1		1	
7– Security considerations	1	5			
TOTAL	23	17		2	

A total of six participants evaluated the USec level of MedHelp and Google Health, according to seven tasks. This provides a total of forty-two participant responses. MedHelp had forty-one however, because one rating was not provided, as mentioned previously. The responses from each OHSN are compared in the graph in figure 6.4. The graph indicates that performing tasks on Google Health's provides more USec than on MedHelp. Following figure 6.4 is a detailed discussion on the tasks and their related scores for each OHSN.

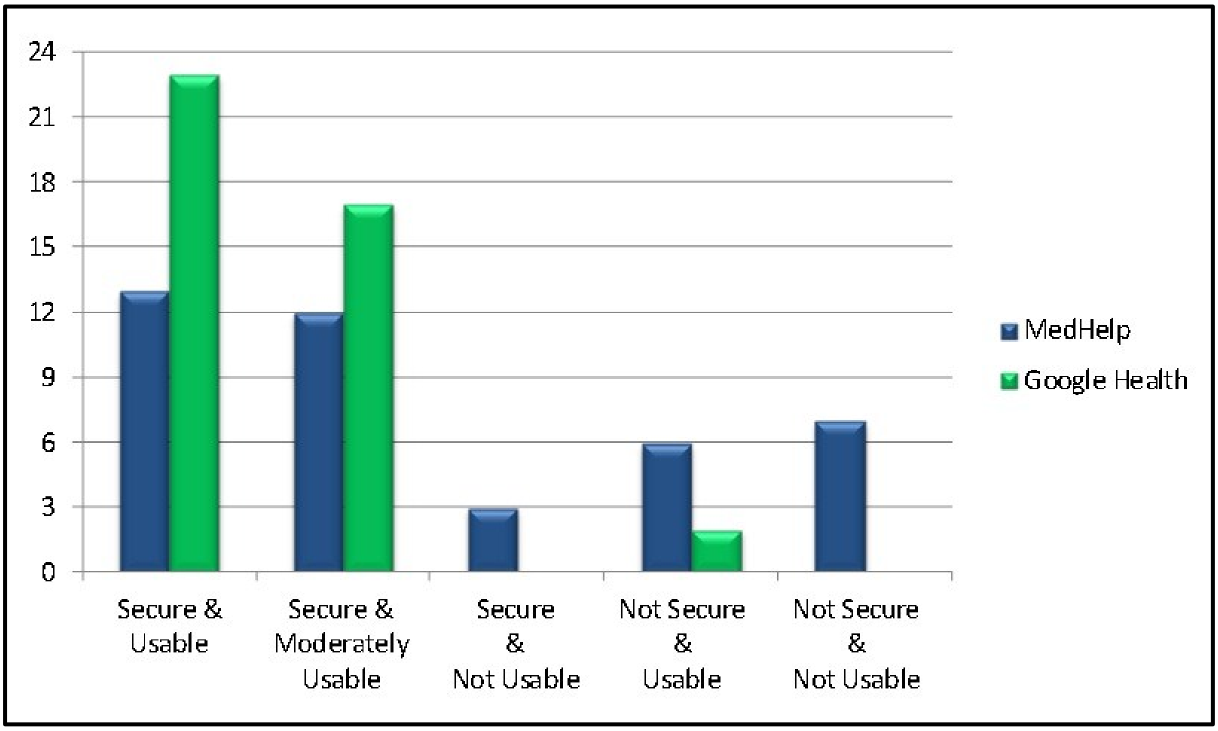


Figure 6.4: Comparison of USec when performing tasks on MedHelp and Google Health

Task 1 refers to the rating of the impression of the homepage. Google Health scored high, as participants trusted it more than MedHelp's homepage. Four scores suggest that the Google Health homepage is *Secure & Usable*; and two scores give *Secure & Moderately Usable*. This is averaged as *Secure & Usable*. MedHelp had two *Secure & Usable*, one *Secure & Moderately Usable* and two *Not Secure & Not Usable* scores. The inconsistency of the scores is of concern. Two scores rated as *Not Secure & Not Usable* cause concern, making it difficult to determine an average for MedHelp.

Task 2 is on the registration process. Google Health scored higher, with five scores for *Secure & Usable*, and one for *Secure & Moderately Usable*, hence averaging *Secure & Usable*. MedHelp had mixed scores, with three *Secure & Usable*, one *Secure & Moderately Usable*, one *Secure & Not Usable* and one *Not Secure & Usable*. The inconsistency should be investigated, even though it averaged a *Secure & Moderately Usable*.

Task 3 focuses on the central place where users configure their security settings. Google Health's My account scored higher than MedHelp's Account settings, having four *Secure & Moderately Usable* and two *Secure & Usable*. Google Health averaged *Secure & Moderately Usable*. MedHelp included two *Secure & Usable*, two *Secure & Moderately Usable* and two *Not Secure & Not Usable*. This makes it difficult to determine an average.

Task 4 focuses on sharing information with other users. Google Health's Share-your-profile rated higher than MedHelp's Find-a-friend. Having five *Secure & Usable* and one *Secure & Moderately Usable* scores, Google Health averaged *Secure & Usable*. MedHelp's mixed scores: two *Secure & Usable*, one *Secure & Moderately Usable*, two *Secure & Not Usable*, and one *Not Secure and Usable* make it difficult to determine an average.

Task 5 focuses on the steps to connect with health-care providers: finding a doctor on MedHelp and importing a medical record in Google Health. Google Health rated slightly higher than MedHelp, with two *Secure & Usable*, three *Secure & Moderately Usable* and one *Not Secure & Usable*. Google Health averaged *Secure & Moderately Usable*. MedHelp had one *Secure & Usable*, three *Secure & Moderately Usable*, one *Not Secure and Usable* and one *Not Secure & Not Usable*. The MedHelp score averaged *Secure & Moderately Usable*.

Task 6 evaluates the online policies. Google Health scored slightly higher than MedHelp, with four *Secure & Usable*, one *Secure & Moderately Usable* and one *Not Secure & Usable*, and a final average of *Secure & Usable*. MedHelp had two *Secure & Usable*, two *Secure & Moderately Usable* and two *Not Secure & Usable*, averaging as *Secure & Moderately Usable*.

Task 7 investigates additional security considerations. Google Health scored higher than MedHelp with one *Secure & Usable* and five *Secure & Moderately Usable*; consequently, it averaged *Secure & Moderately Usable*. MedHelp had one *Secure & Usable*, two *Secure & Moderately Usable*, one *Not Secure & Usable* and one *Not Secure & Not Usable*. This made it difficult finding an average for MedHelp.

Google Health provides more USec than MedHelp in performing security tasks. For Google Health, homepage impression, registration, sharing-your-profile and online policies were *Secure & Usable*. Configuring security settings (via My account), importing-a- medical record and security considerations were rated *Secure & Moderately Usable*. Thus these require improvements in the usability component, as security is deemed adequate.

MedHelp rated poorly against Google Health in terms of USec when performing security-related tasks. For MedHelp, registration process, finding-a-doctor and online policies rated: *Secure & Moderately Usable*. The security/privacy features to perform these tasks need usability improvements. The tasks of homepage impression, security settings (via Account settings), find-a-friend and security were inconclusive because of inconsistency in ratings. This requires investigation. The problem may be in a lack of security, usability, or both; thus, improvements are needed.

6.3.1.5 Recommendations

Recommendations for improving the usability of security and privacy on both OHSNs are provided, according to the usability criteria (Yeratziotis et al., 2011b). Table 6.8 provides recommendations for MedHelp and table 6.9 for Google Health.

Table 6.8: USec recommendations for MedHelp

Usability criteria	**MedHelp recommendations**
Trust	1. Provide mechanisms to verify doctor credibility (e.g. articles, real-life stories, ratings, patient reviews and testimonials). However, this can raise extra privacy issues as users are not using real names either. Provide Google links where users can download additional information about the doctor. Provide confirmation of doctor credentials by university or work institution. Provide a mechanism for doctors to verify their own credibility when they register on the website. 2. Only permit single sign-in sessions. 3. Ensure the verification of email accounts before users are granted access to the website. 4. Provide codes that verify health information. These must be explained and be easily identifiable on the interface (e.g. MedHelp complies with the HON Code. However, users were not aware of it and it was also difficult to identify on the interface. A participant that was aware of it still did not trust it because it is verified by a non-profit organisation. Include additional codes e.g. HIPAA). 5. Provide valid certificates on the website. 6. Provide more security information (e.g. last account activity session and signalling the IP address from which the account is accessed). 7. Users who log out should not be able to return to the previous page by clicking the back button of their browser. 8. Provide less advertising on the website. 9. Consider providing a minimum registration fee for users to join the website. 10. Make security and privacy features more visible on the homepage. Apart from the log-in feature, security policies are hidden in an overpopulated interface, making them difficult to identify. 11. Provide users with a choice for setting an idle log-out time that they deem secure and usable. This will ensure a session lock after a period of inactivity (e.g. similar to time-out sessions on e-banking websites). 12. Provide default settings that are the most advantageous to the user. 13. Users should not need to provide a reason for deleting their account. It

Usability criteria	**MedHelp recommendations**
	should be optional, in case they wish to do so.
Ease of use	1. Provide more information regarding the purpose of a function (e.g. block-list, privacy features). 2. Provide reasoning when a user has been blocked. 3. Reposition the Account settings link either to the top right-hand corner of the interface (next to the logout link) or provide a tab for Account settings instead of a link (similar to the My Home and Profile tabs). 4. The purpose of the Block-list function is explained when users hover over a question mark next to it with the mouse pointer. Novice users may not foresee such an action in order to get this information.
Terminology	1. Provide a checkbox for users to select when stating that "*I accept the terms and conditions*". 2. Provide shorter sentences in policies. Some are too long, which makes reading and understanding them difficult. 3. Provide policies with simpler language. They currently read like legal documents, which are difficult to understand. However, this is their purpose and it is standard practice. It may be useful to consider simpler version policies in addition to the legal ones. 4. Key points are not revealed regarding what will be released and how information will be used, although they indicate what information will not be used for (e.g. Disclosure to third-party advertising companies, privacy concerns to connect with Facebook).
Ease of learning	1. The text size for the Account settings sub-links are too small in comparison to other text on the interface, which makes them difficult to identify. 2. Provide the procedure for verifying the email address in the Notifications sub-link. 3. Provide better descriptions for actions and features. These are not clear for first time users. 4. Provide distinct boundaries for sub-links. Users cannot always determine in which sub-link they are visually.
Feedback	1. Confirm changes more visibly. Identification is difficult because they are not at the point of recent activity (e.g. change password, change privacy settings). 2. Once users change their nickname (as requested by the website), the notification message remains, even if the nickname has been successfully changed. Only when users select signup is it removed. 3. The website delays notifying users if a nickname is in use. In addition, suggested nicknames are difficult to remember, even though they are difficult to guess and are "close" to users' initial preferences. 4. Provide emails to verify the change of password. 5. The "change password" window must be closed once the process is complete and confirmation is provided. 6. Provide a current status when sending an invite to a friend (e.g. pending reply).

Usability criteria	MedHelp recommendations
Awareness	1. The details of the user who is logged-in must be more visible. It is difficult to identify because of location and text size. 2. It is not apparent that the Account Settings link refers to the security and privacy settings of the user profile. 3. Users are not made aware of the consequences of unblocking another user. They are only provided with a pop-up screen asking them if they are sure about this action. 4. Provide more information about friend invitation requests when accessing the Friends link. 5. There is no confirmation that friend invitation requests have been sent. The only time it is observable is when the user selects the Invite button. 6. Provide more options and descriptions in the Account settings link instead of sub-links (similar to Facebook).
Errors	1. Provide more guidance in error messages (e.g. where a password does not match confirmation password, try providing a solution to the problem as well, such as Caps Lock is active). 2. When a user enters an incorrect verification code during registration, the website fails to generate a new one.
Help & documentation	1. Provide more information about security, privacy and confidentiality in the FAQs (e.g. Is my information safe? Who can view my account? Who is the custodian of my information? What happens with my information when I deregister? Do third-party websites access my information? Are the doctors credible?) 2. Provide more guidance on how a user can link their profile to their Facebook account and how Facebook benefits from this.

Table 6.9: USec recommendations for Google Health

Usability criteria	Google Health recommendations
Trust	1. Provide more country-specific policies. Security/privacy issues tend to be well presented but are the same, regardless of the users' country of origin (selected when users create their profile). In addition to general website policies, there could be supplementary ones specific to the country of origin. These must also be provided in the native languages, along with English. 2. Provide more information and reviews about the third-party websites that deliver additional health services. This includes criteria for including them in Google Health. Because Google Health states that it is the sole responsibility of the user to review and approve the third-party service, trust is reduced. 3. Provide codes that verify health information (e.g. Department of Health, HIPAA, HON Code). 4. Only permit single sign-in sessions. 5. The identity signal should be retained in the Privacy Principles window, even though it appears on the main Google Health window. This shows

Usability criteria	Google Health recommendations
	inconsistency in presenting security information. 6. Provide users with a choice for setting an idle log-out time that they deem secure and usable. This will ensure a session lock after a period of inactivity (e.g. similar to time-out sessions on e-banking websites).
Ease of use	No recommendations.
Terminology	1. Re-phrase the statement "*By clicking on 'I accept' below you are agreeing to the Terms of Service above and the Privacy Policy*". 2. Provide an additional policy for Google Health and third-party websites that clearly states the responsibilities and services of each. 3. Provide explicit measures stipulating privacy and security guarantee of users' personal information.
Ease of learning	1. Provide more icons. Users should have the option to use a text- or icon-based interface. Currently, it is very text-based. 2. Verifying an email account must be simple and clear to the users. When users register, the status of their account is displayed as not verified, with no additional instructions.
Feedback	1. Even though feedback is generally identifiable, providing it in pop-up messages and in a larger text may increase usability. 2. Regarding the Show activities tab, brief descriptions are required to further improve understanding. 3. Provide a mechanism to check for email account availability during registration. This can provide instant feedback.
Awareness	1. Provide more information about the private lock icons on the users' profile page. The participants guessed what the icons meant. They also stated that their field knowledge allowed them to understand what the icons referred to, but they need to be made clearer for other users. 2. Provide more information about the purpose of the Activity report function. 3. Make it clearer that the My account function can be used by users to configure the security and privacy settings of their profile. 4. Provide a setting for users whereby they may customise the expiry date in the Share with others function. This relates to sharing their profile with another user.
Errors	1. During the registration process, users are required to submit the page before receiving any error messages (e.g. mismatch in password and confirmation password or incorrect verification code). Usability would be increased if the system were to notify the user that there is an error in the current input field before the user moves to the next one. 2. Mandatory fields are not displayed during the registration process. This can limit the possibility of a potential error (e.g. users are forced to re-enter information because the field is left blank in the initial registration process). 3. When users select to search for updates, an error occurs and no information is provided regarding the problem or the solution.
Help & documentation	1. Provide more information about the security and privacy of users' personal health information on the Privacy Centre page. This applies to the Help Centre page as well (e.g. Security of my account, health information, my information when I delete my account).

Recommendations for both the OHSNs are based on the participants' feedback. The scenarios provided to the participants' helped create a mental model regarding the experiences of a typical user. All tasks conducted related to security and privacy interactions as well as the concerns that a user would experience when using the particular OHSN.

6.3.2 Data Collection Method II – Heuristic Evaluation

Once the participants' had completed their tasks, they used the USec HE to evaluate the OHSN, as discussed in section 5.5.8.4. A task could comprise a number of subtasks, which would inform specific checklist items from the USec HE. These demonstrated the way in which the specific subtask is addressed by a checklist item in the USec HE, with most subtasks having corresponding checklist items for their evaluation. Each user had tasks and subtasks for MedHelp and Google Health. *Appendix B.2: Scenarios and Tasks (MedHelp)* and *Appendix B.3: Scenarios and Tasks (Google Health)* present the tasks that participant 1 conducted on each of these respectively. It also includes the participant's comments and answers to questions. Similarly, appendices B.9 and B.10 present the views of participant 2 on MedHelp and Google Health respectively. Appendices B.16 and B.17 present the views of participant 3, appendices B.23 and B.24 present the views of participant 4, appendices B.30 and B.31 present the views of participant 5 and appendices B.37 and B.38 present the views of participant 6.

The HE included a column in which participants' could provide additional comments, although this was optional. Any comments made could relate to the OHSN, the checklist item or both. Table 6.10 summarises the checklist items for which the participants' provided negative, yet constructive comments, which identified problems. These should be considered in the next iteration in order to improve the USec HE. The frequency with which a problem was identified is also presented in the table.

Table 6.10: Participant issues with checklist items

Checklist Item	Problem and Recommendations	Task
1.2 If pop-up windows are used to display security-related error messages, do they allow the user to see the field in error?	a) This item should be rephrased	a) 1
4.1 Are users initiators of security actions rather than respondents?	a) Confusion between the words "users'" and "respondents"	a) 1
5.1 Have security items been grouped into logical zones, and have headings been used to distinguish between the zones?	a) Disagreement with categorisation of checklist item under heuristic	a) 1
6.1 Is only the security information essential to decision making	a) Difficult to understand item	a) 1

Checklist Item	Problem and Recommendations	Task
displayed on the screen?		
6.4 Are security prompts expressed in the affirmative?	a) Suggested examples of prompts be provided	a) 1
8.3 Do security-related prompts imply that the user is in control?	a) Suggested examples of prompts be provided	a) 1
11.3 Can users switch easily between security help and their work?	a) The word "work" is vague	a) 1
11.4 Do instructions follow the sequence of user security actions?	a) Depends on what the user needs to do since there are lots of alternatives in different situations.	a) 1
11.5 Does the system provide users with updated security educational opportunities, if they desire it?	a) Difficult to understand item	a) 1
13.2 Can protected or confidential areas be accessed with certain passwords?	a) The word "certain" password is vague b) Difficult to understand item	a) 2 b) 3
13.11 Are notification messages relating to security and privacy displayed to the user before access to the system is granted?	a) The phrase "Are notification messages" is vague b) Not clear if notification messages includes pop-up message boxes	a) 1 b) 1
13.15 Does the system employ automated tools that provide notification to the user upon discovering discrepancies during integrity verification?	a) Difficult to understand item	a) 3

The issues with the USec HE, as identified by the participants, are presented in table 6.10. To address these, not only the problems in the websites should be considered, but also and more importantly, the process for developing heuristics for SADs should be addressed. This allows one to determine where modifications are necessary and subsequently iterate back to a relevant task that can solve an issue. Firstly, the phase of iteration must be determined. Following this, the task within the phase that relates to the specific problem is identified. In this case, all issues will be addressed in phase 1. This is because phase 1 focuses on the design of the high-level heuristics. Problems relating to the validation of the high-level heuristics or the application of them in a context would have been addressed in phases 2 and 3 respectively.

The next step is to determine in which task of phase 1 a participant issue can be resolved. This is presented in table 6.11. The checklist item and problem columns are the same as in table 6.10. Therefore, just the number of the checklist item and the problem letters is provided in table 6.11.

Table 6.11: Tasks of phase 1 where participant issues can be addressed

Checklist item	Problem	Task
1.2 , 4.1, 6.1, 6.4, 8.3, 11.3, 11.5 & 13.15	a)	a) 2 – Name high-level heuristics according to themes identified
5.1	a)	a) 4 – Group checklist items based on high-level heuristic names
11.4	a)	a) 1 – Review literature
13.2 & 13.11	a) b)	a) 2 – Name high-level heuristics according to themes identified b) 2 – Name high-level heuristics according to themes identified

It is clear from table 6.11 that most issues relate to the wording of items in the HE checklist; making the terminology clearer and understandable. The problem with checklist 5.1 relates to its categorisation under a heuristic name and the problem with checklist item 11.4 is that it is context dependent. All items present areas for possible modifications that can improve the USec HE.

The checklist items have been modified to address the participant concerns. The modified version of the USec HE is presented in chapter 8. It is also worth mentioning that the sequence of the heuristics and their checklist items differed during the evaluations with participants'. The reason for this was to associate the sequence of tasks and subtasks in the scenarios and tasks manuscript with the order of heuristics and their checklist items in the USec HE. This would make it easier for participants' to complete tasks and then evaluate them with relevant checklist items. *Appendix B.4: USec HE (MedHelp)* and *Appendix B.5: USec HE (Google Health)* present the results from the HEs that participant 1 conducted on each of these OHSNs respectively. Similarly, appendices B.11 and B.12 present the HEs of participant 2 on MedHelp and Google Health respectively. Appendices B.18 and B.19 present the HEs of participant 3, appendices B.25 and B.26 present the HEs of participant 4, appendices B.32 and B.33 present the HEs of participant 5 and appendices B.39 and B.40 present the HEs of participant 6.

6.3.3 Data Collection Method III – User Satisfaction Questionnaire

The final method used in the case study was a user satisfaction questionnaire, as mentioned in section 5.5.8.2. This followed the HE that the participants conducted on each OHSN. The questionnaire included fifteen items and focused on the users' reviews regarding the application and usage of the USec HE as a tool for assessing the level of USec in the two OHSN. Table 6.12 summarises the frequencies of the participants' responses (n = 6). In table

6.12 the scores for questions 1 to 13 are representative of the number of participants that selected the following: SA = Strongly Agree; A = Agree; U = Undecided; D = Disagree; and SD = Strongly Disagree.

The scores for question 12 are representative of the number of participants that selected the following: VI = Very Important; I = Important; MI = Moderately Important; OLI = Of Little Importance; and U = Unimportant.

The scores for questions 13 - 14 are representative of the number of participants that selected the following: VG = Very Good; G = Good; BA = Barely Acceptable; P = Poor; and VP = Very Poor. Table 6.12 is followed by an analysis of the questions and their related scores.

Table 6.12: Overall ratings from user satisfaction questionnaire

#	Question	SA	A	U	D	SD
1	I can evaluate a security and privacy feature quickly applying the checklist items.		6			
2	I am satisfied with the number of checklist items included.	1	4		1	
3	The length of the USec HE should be shortened.	2	2	2		
4	It is easy to understand how to apply the USec HE.		5	1		
5	The heuristic descriptions clearly describe what the checklist items are evaluating.	1	5			
6	The terminology used in the USec HE is clear and easy to understand.	1	5			
7	I would need additional instructions to evaluate a website with the USec HE.		2		4	
8	It is easy to learn how to use the USec HE once you have used it once.	3	2	1		
9	Checklist items are well categorised under a heuristic.	1	4	1		
10	The amount of information included in the USec HE was useful.	1	4	1		
11	The use of the USec HE is complex		1	1	4	
#	**Question**	**VI**	**I**	**MI**	**OLI**	**U**
12	Developing tools that improve the usability of security and privacy features.	4	2			
#	**Question**	**VG**	**G**	**BA**	**P**	**VP**
13	Overall, how would you rate the quality of the USec HE?	1	5			
14	Overall, how would you rate the effectiveness of the USec HE?		5	1		

Question 1 examined the time required to evaluate security and privacy features on a website using the USec HE. All participants *Agree* that the evaluation can be done quickly by applying the relevant checklist items.

Question 2 examined the participants' satisfaction with regard to the number of checklist items included in the USec HE. Results show one *Strongly Agree*, four *Agree* and one *Disagree* with regard to their satisfaction. Overall, participants were satisfied with the number of checklist items included.

Question 3 examined the length of the USec HE. This question relates directly to Question 2. The results show that two participants *Strongly Agree*, two *Agree* and two are *Undecided* with regard to shortening the length of the HE. The results contradict those in Question 2. Therefore, the length of the HE and the number of checklist items within it is an area that requires more attention in the next iteration phase.

Question 4 examines the ease of use of the USec HE. The results show that overall participants felt that the tool was easy to use. Five participants *Agree* and one is *Undecided* that it is easy to understand how to apply the tool during evaluation.

Question 5 examines the descriptions of the heuristics. Each heuristic consists of a name and an associated description. Categorised under the heuristic name are relevant checklist items that operationalise it. This assists experts in understanding its application in context. Generally, participants felt that the heuristic descriptions adequately describe what their associate checklist items evaluate. Results show one *Strongly Agree* and five *Agree* on this level.

Question 6 relates to the terminology used in the USec HE. Overall, participants were satisfied with the language and the results show one *Strongly Agree* and five *Agree* scores regarding clear and easy-to-understand terminology.

Question 7 examined the instructions that were provided for the USec HE. The consensus was that the instructions are sufficient. It should be noted that the instructions and design of the USec HE were based on well-recognised and applied HEs. These include the Xerox HE system checklist and Jakob Nielsen's severity ratings. The results show that two participants *Agree* and four *Disagree* regarding additional instructions to conduct an evaluation.

Question 8 examined the ease of learning to use the USec HE. This is important because experts should remember how to reuse the tool in subsequent evaluations. Results show that three participants *Strongly Agree*, two *Agree* and one is *Undecided* about the tool being easy to remember how to use. Generally, it is regarded as a tool that is easy to remember how to use.

Question 9 examines the categorisation of checklist items under their heuristics. This question relates directly to Question 5. The results show that the checklist items are well categorised, as one participant answered *Strongly Agree*, four *Agree* and one *Undecided* for this. These results are further confirmed, as the results from this question correlate with those of Question 5.

Question 10 examines the usefulness of the amount of information provided in the USec HE. This ensures that the participants are satisfied that the information in checklist items is useful for determining security/privacy usability violations on websites and applications. Generally, the results show that participants felt that the information is useful, as one answered *Strongly Agree*, four *Agree* and one *Undecided* for this question.

Question 11 examines the complexity involved in using the USec HE. This question directly relates to Question 4 and there is a correlation between the results of both questions. In regard to question 11, the results show that one participant answered "Agree", one "Undecided" and four "Disagree" that it is a complex tool to use.

Question 12 was not directly focused on the USec HE. Instead, it required the participants' opinions concerning the development of USec tools. Since they had the opportunity to assess the level of USec on the two OHSNs using the available tool, they could provide an informed opinion. Their opinions were grounded on their experiences as users, utilising the security/privacy features of each website. The results show that four participants stated that it is *Very Important* and two that it is *Important* to develop tools that improve the usability of security and privacy features for users. This helps to justify the contribution of the proposed tool and the research.

Question 13 examined the overall quality of the USec HE. The tool can be regarded as being of good quality, as one participant rated it *Very Good* and five rated it *Good*. However, this does suggest that the tool could be further improved.

Question 14 examined the overall effectiveness of the USec HE. The overall effectiveness of the tool was deemed satisfactory, as five rated it *Good* and one rated it *Barely Acceptable*. Of concern is the *Barely Acceptable* rating. Once again, the results suggest that the tool can be further improved.

Question 15, which is not included in table 6.12, was an optional question. Participants could provide suggestions for improving the USec HE. Accordingly, one participant suggested reducing the length of the tool, which was confirmed by the results of Question 3.

To summarise, the only real concern that might require improvement in the next iteration of the tool is its length, which needs to be reduced. The effectiveness and quality of the tool is more than satisfactory. This is positive and suggests that the tool is successful in achieving its intended objectives. However, it would be worthwhile in future research to examine where further improvements could be made to improve quality and effectiveness.

6.4 SUMMARY

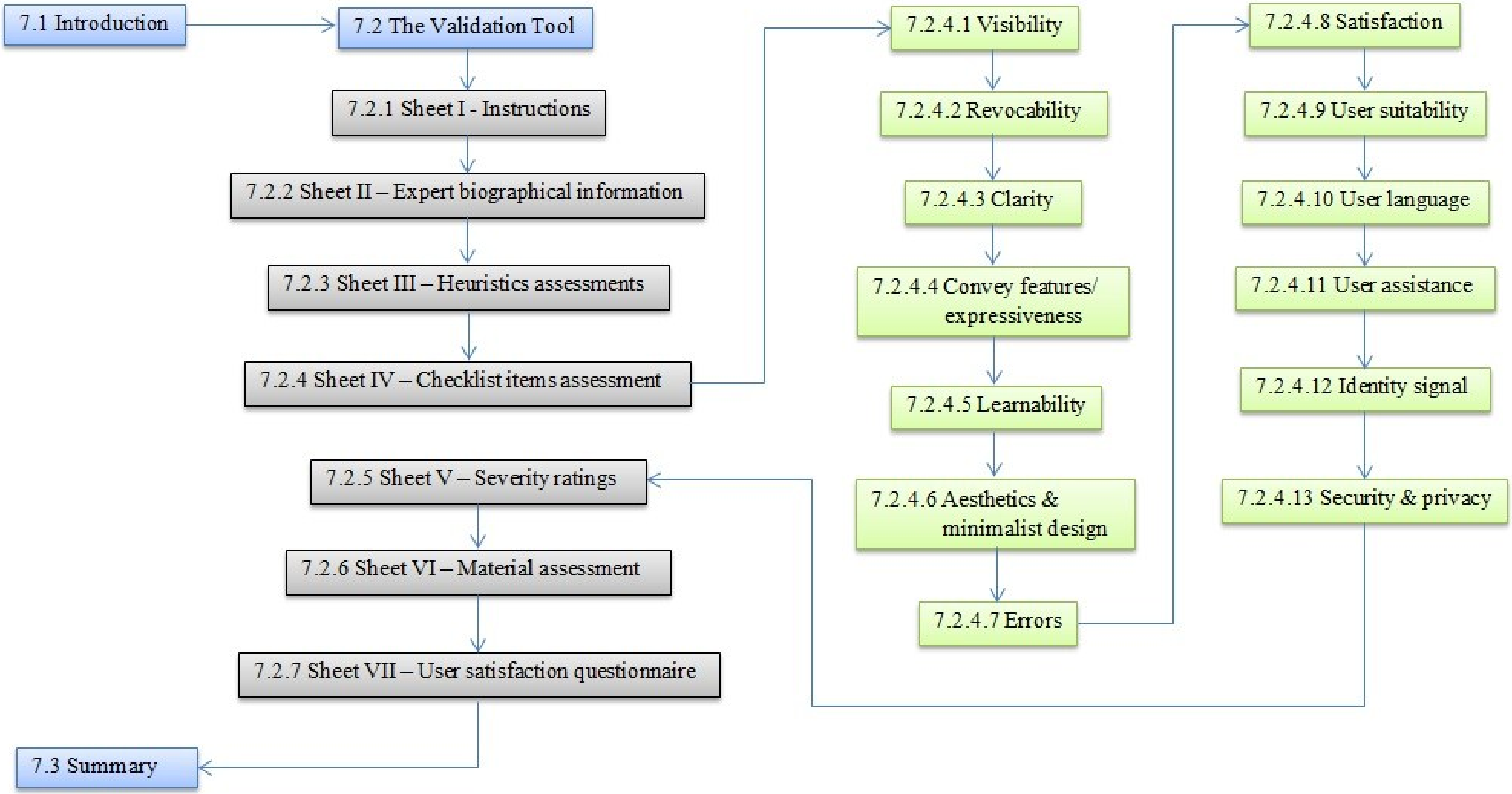
This chapter began by discussing OHSNs and provided an overview of the environment (or context) in which the USec HE was applied. Upon introducing the OHSNs, PHI was mentioned – the essence of an OHSN. A discussion followed on their themes and capabilities, whereupon the focus moved to barriers and concerns for the adoption of OHSNs. In addition, the semantic Web was introduced and its potential role and impact on the medical field was highlighted.

The chapter then focused on the case study. The first method used in the case study, the formative usability method, was initially discussed. This included discussions on the selected OHSNs, the participants, scenarios and tasks. The results and analysis from the evaluations followed. These results were based on two factors: evaluating the security and privacy features of the OHSNs by applying usability criteria and evaluating the tasks that participants' performed by applying USec ratings. Regarding their security and privacy features, results indicated that Google Health had higher levels of usability in comparison to MedHelp. Regarding the tasks performed, results indicated that Google Health provided more USec than MedHelp. Analogous recommendations were then made for improving both OHSNs.

This was followed by a discussion on the second method, the HE. Participants' evaluated the OHSNs with the USec HE after they had completed their FUE. They then provided feedback relating to both the OHSNs and the USec HE. Regarding the USec HE, twelve possible areas for improvement were identified. These included checklist items 1.2, 4.1, 5.1, 6.1, 6.4, 8.3, 11.3, 11.4, 11.5, 13.2, 13.11 and 13.15. It must be clarified that participants applied the USec HE after first iteration during the FUE, as presented in table 4.3 (despite its modification to associate the tasks and subtasks with heuristics and checklist items, as mentioned in section 6.3.2). The improved USec HE after second iteration is based on the participants and experts feedback and is presented in table 8.2.

The final method used in the case study was a user satisfaction questionnaire, in terms of which participants' provided their overall opinions about the USec HE. Based on the results, it is concluded that the USec HE is an effective tool that can achieve its objectives. However, the length of the tool should be reduced. In chapter 7 the results and analysis from the experts' validations are presented.

LAYOUT OF CHAPTER 7


7.1 Introduction
7.2 The Validation Tool
7.2.1 Sheet I - Instructions
7.2.2 Sheet II – Expert biographical information
7.2.3 Sheet III – Heuristics assessments
7.2.4 Sheet IV – Checklist items assessment
7.2.4.1 Visibility
7.2.4.2 Revocability
7.2.4.3 Clarity
7.2.4.4 Convey features/ expressiveness
7.2.4.5 Learnability
7.2.4.6 Aesthetics & minimalist design
7.2.4.7 Errors
7.2.4.8 Satisfaction
7.2.4.9 User suitability
7.2.4.10 User language
7.2.4.11 User assistance
7.2.4.12 Identity signal
7.2.4.13 Security & privacy
7.2.5 Sheet V – Severity ratings
7.2.6 Sheet VI – Material assessment
7.2.7 Sheet VII – User satisfaction questionnaire
7.3 Summary

CHAPTER 7: RESULTS AND ANALYSIS FROM VALIDATION TOOL

7.1 INTRODUCTION

This chapter will discuss the assessments that were conducted by the experts, who used a validation tool to assess the USec HE. In addition, assessment criteria were established to evaluate the heuristics and their checklist items. Other factors that impact on the validity of the USec HE were also evaluated; these also form part of the validation tool and will be discussed in this chapter. Section 7.2 will analyse and discuss the results of the validations and a summary is presented in section 7.3.

7.2 THE VALIDATION TOOL

The validation tool was designed in MS Excel and comprised seven sheets (or sections). These included instructions, expert biographical information, heuristics assessments, checklist items assessment, severity ratings, material assessment and a satisfaction questionnaire. Each of these will be discussed in more detail in their respective sections within this chapter. The validation tool is presented in *Appendix A.2: Validation Tool Template*. The complete ratings of the four experts are also available in the appendices. *Appendix C.1: Validation Tool of Expert 1* presents the ratings of expert 1. Similarly, appendix C.2 presents the ratings of expert 2, appendix C.3 presents the ratings of expert 3 and appendix C.4 presents the ratings of expert 4.

7.2.1 Sheet I – Instructions

This sheet was used to explain the nature of an HE to the experts and how it can be used to evaluate an interface for usability violations. It then mentioned the purpose of the validation tool and the fact that it would be used to assess a new set of USec heuristics. In addition, experts were provided with the complete USec HE in a PDF format. This was provided for viewing purposes so that they could have a better understanding of the "look and feel" of an HE. Specific instructions were also provided for each sheet. These were available on the actual sheet.

7.2.2 Sheet II – Expert Biographical Information

This sheet was used to record the biographical details of the experts and was important to determine the level of expertise that each of the experts possessed in terms of the three fields of USec, HCI and InfoSec. This would help measure their comments or feedback for the modifications that are provided in the validation tool and would contribute to understanding the perspective from which they give their opinions and how they rate in terms of their level of skill in the other fields. Other biographical information was also collected. Selected details of the experts' biographical information are summarised in table 7.1.

Table 7.1: Expert profiles

	Expert 1	**Expert 2**	**Expert 3**	**Expert 4**
Country	South Africa	UK	Zimbabwe	China
Occupation	Academic	Academic	Academic	Academic
Industry	IT	Education	Education	Education
Experience (years)	15	30	6	29
HCI experience	Intermediate	Expert	Intermediate	Expert
InfoSec experience	Expert	Expert	Expert	Intermediate
USec experience	Intermediate	Expert	Intermediate	Intermediate

Table 7.1 thus indicates that two of the experts were HCI experts, three were InfoSec experts, and one was a USec expert. One of them can be considered as a "triple-expert", with expertise in all three fields.

7.2.3 Sheet III – Heuristics Assessments

The focus of this sheet was to assess the high-level heuristic names together with their descriptions. These form the "groups" into which relevant checklist items would be categorised. The development of the high-level heuristics and their descriptions were discussed in section 4.4. This sheet specifically addressed the importance and clarity of name and description. Experts could also provide optional comments were they felt necessary. One expert did not provide an importance rating for heuristic 6. Hence there are in total thirteen high-level heuristics for USec. Tables 7.2 and 7.3 summarise the frequencies of the experts' responses (n = 4) for the importance and clarity of the high-level heuristics. In table 7.2 the scores are representative of the number of experts that selected the following: VI = Very Important; I = Important; MI = Moderately Important; OLI = Of Little Importance; and NI = Not Important. The total for the responses are accumulated for each score, as well in both tables.

Table 7.2: Overall ratings for the importance of the USec high-level heuristics

#	**Heuristic**	**VI**	**I**	**MI**	**OLI**	**NI**
1	Visibility	2		2		
2	Revocability	3		1		
3	Clarity	3	1			
4	Convey Features/Expressiveness		1	2	1	
5	Learnability	3		1		
6	Aesthetics and Minimalist Design	1	1	1		
7	Errors	4				
8	Satisfaction	2	1			1
9	User Suitability	3		1		
10	User Language	4				
11	User Assistance	3	1			
12	Identity Signal		3			1
13	Security and Privacy	2	2			
TOTAL		30	10	8	1	2

The purpose of the importance rating was to determine whether any heuristics can be eliminated from the final USec HE. To retain a heuristic, the average of the experts' responses must infer that it is either a *Very Important* or an *Important* heuristic for the USec HE.

It was decided that the visibility heuristic would be retained as two experts rated it as *Very Important* and two as *Moderately Important*. This confirms that it is an essential heuristic for USec. The first *Moderately Important* score was awarded by an InfoSec expert, who also added that a balance is required in terms of the security status information provided to a user. This should keep a user informed, but it should not confuse or frighten (e.g. if the user status is moderately secure and not fully secure). The second *Moderately Important* score was awarded by a USec expert with no additional comments.

The revocability heuristic would be retained as three experts rated it as *Very Important* and one as *Moderately Important*. This confirms that it is an essential heuristic for USec. The *Moderately Important* score was awarded by an InfoSec expert and the score can be justified by the comments of the USec expert, who stated that revocability is required but within reason. There are security actions where revocability should not be permitted (e.g. revoking the security code of a credit card to authorise an online payment). That being said, revocability can be applied to many other security actions that a user performs (e.g. revoke a login, revoke access to information).

The clarity heuristic would be retained, as three experts rated it as *Very Important* and one as *Important*. This confirms that it is an essential heuristic for USec. The *Important* score was awarded by an InfoSec expert.

The convey features/expressiveness heuristic was awarded the lowest scores on average. One expert rated it as *Important*, two as *Moderately Important* and one as *Of Little Importance*. The scores suggest that this heuristic is not essential and could therefore be eliminated from the USec HE. The two *Moderately Important* scores were awarded by the one InfoSec and HCI experts, while the USec expert rated it as *Of Little Importance*. There was thus consensus among the experts in each field that it is not an indispensable heuristic.

The learnability heuristic would be retained as three experts rated it as *Very Important* and one as *Moderately Important*. This confirms that it is an essential heuristic for USec. The *Moderately Important* score was awarded by the USec expert.

The aesthetics and minimalist design heuristic had mixed scores. The USec expert did not provide a rating for this heuristic. However, the scores included one *Very Important* from an InfoSec expert, one *Important* from the HCI expert and one *Moderately Important* from the second InfoSec expert. Hence, the results suggested that it is an essential heuristic for USec and it would therefore be retained. The rating of the HCI expert is supported by those of the InfoSec experts.

The errors heuristic would be retained as all four experts rated it as *Very Important*. This confirms that it is an essential heuristic for USec. However, the USec expert raised the concern that, despite the heuristic's evident importance, error messages might benefit attackers as much as the intended users.

The satisfaction heuristic would be retained as two experts rated it as *Very Important*, one as *Important* and one as *Not Important*. This confirms that it is an essential heuristic for USec. The *Not Important* score was awarded by the USec expert, who added that users cannot be in control of security, rather it is the system that controls security. The HCI expert rated it as *Very Important*, while the two InfoSec experts rated it as *Very Important* and *Important* respectively. Taking into account the overall scores, it was decided to retain this heuristic, despite the strong argument of the USec expert.

The user suitability heuristic would be retained as three experts rated it as *Very Important* and one as *Moderately Important*. This confirms that it is an essential heuristic for USec. The *Moderately Important* score was awarded by the HCI expert. One InfoSec expert supported this heuristic by agreeing that novice users should be provided with less security information in comparison to the more advanced users.

The user language heuristic would be retained as all four experts rated it as *Very Important*. This confirms that it is an essential heuristic for USec. No additional comments were made by the experts in terms of this heuristic.

The user assistance heuristic would be retained as three experts rated it as *Very Important* and one as *Important*. This confirms that it is an essential heuristic for USec. The *Important* score was awarded by an InfoSec expert.

The identity signal heuristic would be retained as three experts rated it as *Important* and one as *Not Important*. This confirms that it should be included in the USec. The *Not Important* score was awarded by the USec expert who also stated that research proves users do not take note of the identity signal and therefore it does not impact on usability. This is a valid argument presented by the expert, which does uphold considering the elimination of the heuristic. The argument is based on two facts; first, users do not use identity signal information because they do not notice it, and second, it is impossible for the identity signal to impact on usability if users are unaware of it in the first place. Therefore, making the identity signal more noticeable on the browser of use should be the first priority, followed by improving its usability thereafter. However, this is beyond the scope of this study. Finally, owing to the fact that the other three experts were in agreement that it is an important heuristic, it is retained.

The security and privacy heuristic would be retained as two experts rated it as *Very Important* and two as *Important*. This confirms that it is an essential heuristic for USec. The *Important* scores were awarded by the one InfoSec expert and the HCI expert. The USec expert rated it as *Very Important*, while adding that ensuring confidentiality, integrity and availability is always maintained is the core goal of all security systems, even though it is probably an unattainable one.

In review, there were a total of four experts who evaluated the 13 high-level heuristics for their level of importance. This provides a total of fifty-two possible responses. One of the experts did not provide a rating for the aesthetics and minimalist design heuristic, resulting in a total of fifty-one expert responses. The totals for each rating per heuristic are listed in table 7.2 and displayed in the graph in figure 7.1.

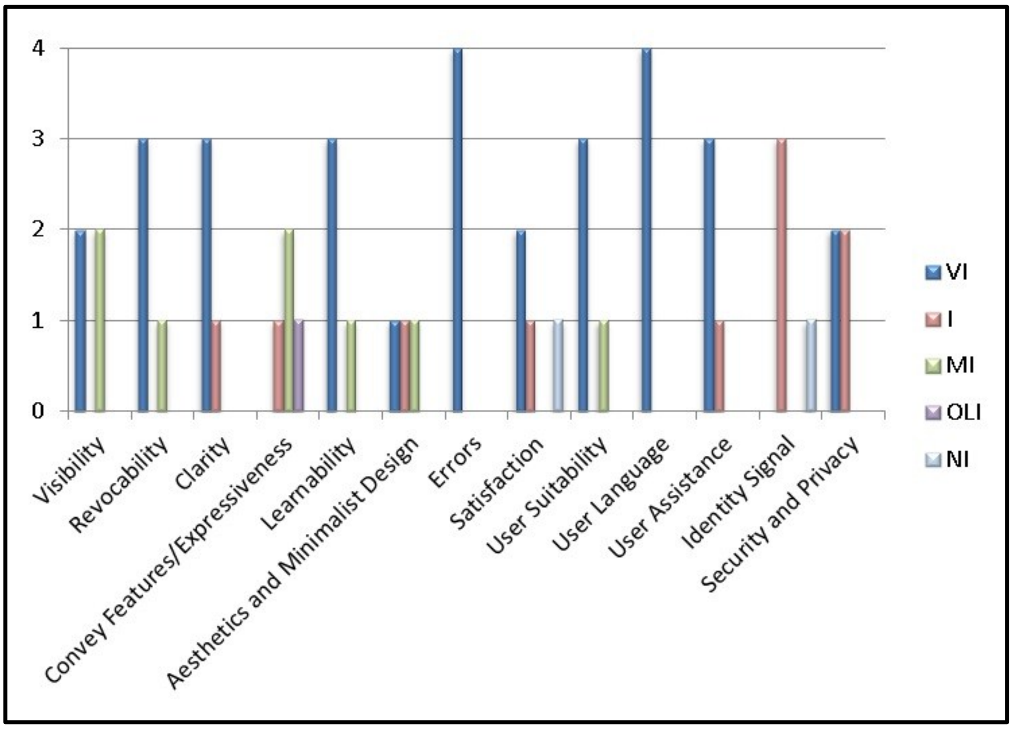


Figure 7.1: Comparison of ratings for the importance levels of each USec heuristic

Table 7.3 focuses on the clarity of the high-level heuristics. This measure assessed if the terminology used for the USec high-level heuristic names and descriptions is unambiguous and easy to understand. The scores are representative of the number of experts that selected the following: VG = Very Good; G = Good; BA = Barely Acceptable; P = Poor; and VP = Very Poor.

Table 7.3: Overall ratings for the clarity of the USec high-level heuristics

#	Heuristic	VG	G	BA	P	VP
1	Visibility – the system should keep users informed about their security status	4				
2	Revocability – the system should allow users to revoke any of their security actions	2	1	1		
3	Clarity – the system should inform users in advance about the consequences of any security actions	4				
4	Convey Features/Expressiveness – the system should guide users on security in a manner that still gives them freedom of expression	1	2	1		

#	Heuristic	VG	G	BA	P	VP
5	Learnability – the system should ensure that security actions are easy to learn and remember	4				
6	Aesthetics and Minimalist Design – the system should offer users relevant information relating to their security actions	2		1	1	
7	Errors – the system should provide users detailed security error messages that they can understand and act upon	3	1			
8	Satisfaction – the system should ensure that users have a good experience when using security and that they are in control	3	1			
9	User Suitability – the system should provide options for users with diverse levels of skill and experience in security	3	1			
10	User Language – the system should use plain language that users can understand with regard to security	4				
11	User Assistance – the system should make security help apparent for users	3	1			
12	Identity Signal – the system should have valid certificates and the information should be available on the browser of use	1	3			
13	Security and Privacy – the system needs to consider integrity, availability, confidentiality and privacy		2	2		
TOTAL		34	12	5	1	

The results shown in table 7.3 indicate that improvements can be made to certain heuristics in terms of their clarity. The heuristics that can be improved include the following:

- Revocability – The USec expert rated this *Barely Acceptable*. This could possibly relate to the comment the same expert made when evaluating the importance of this heuristic; that is, security actions can be revoked within reason. This should be depicted in the description.
- Convey features/expressiveness – The USec expert rated this *Barely Acceptable* and stated that the meaning is ambiguous. However, the importance of this heuristic was rated low and it was therefore eliminated from the final USec HE.
- Aesthetics and minimalist design – The USec expert rated this *Poor* because the heuristic name and description do not match, while the HCI expert rated this *Barely Acceptable*. Based on the fact that the HCI and USec expert were not satisfied with the clarity, the description must be revised.
- Errors – When evaluating the importance of the heuristic, the USec expert previously mentioned caution should be exercised in ensuring that error messages do not benefit attackers. Furthermore, the description can denote that users must be told how to recover when possible or what to do when this in not possible.
- Identity signal – The heuristic can be reviewed, even though it has an overall *Good* rating. Only one InfoSec expert rated it as *Very Good*.

- Security and privacy – The heuristic was rated *Barely Acceptable* by the two experts from HCI and USec. The USec expert could not understand the use of the term *consider* within this context. An InfoSec expert addressed this concern and suggested that the term *consider* should be replaced with *ensure* and that what was mentioned previously be included to ensure that confidentiality, integrity and availability are the goals, even though they are perhaps unattainable.

In review, a total of four experts evaluated the 13 high-level heuristics for level of clarity. This provides a total of fifty-two possible responses. The totals for each rating per heuristic are listed in table 7.3 and displayed in the graph in figure 7.2.

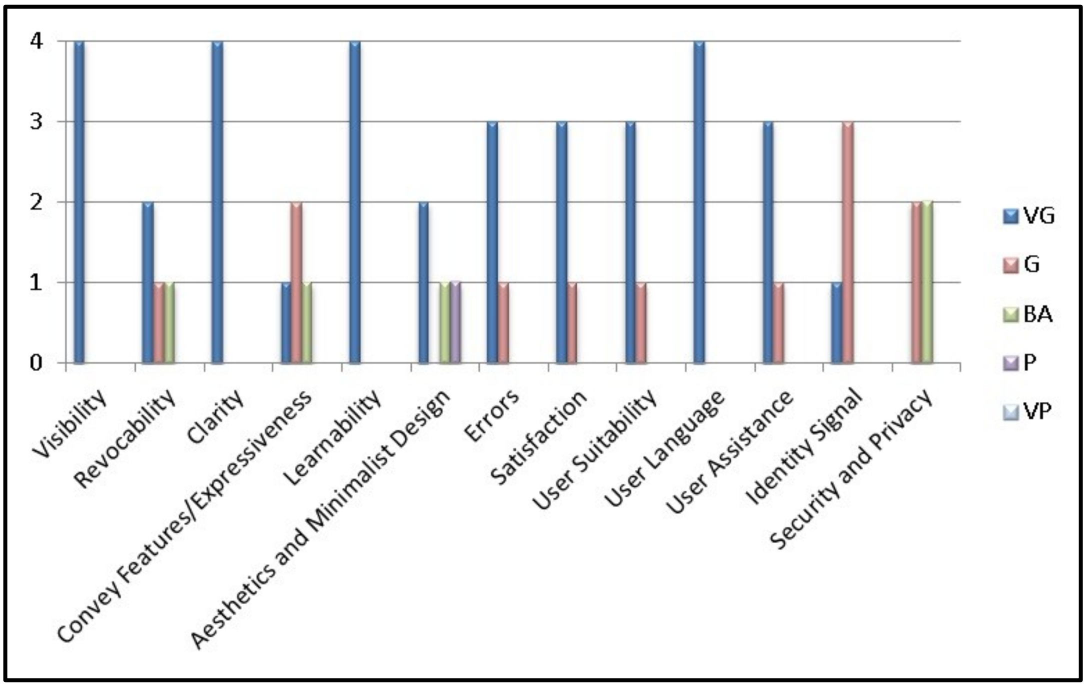


Figure 7.2: Comparison of ratings for the clarity levels of each USec heuristic

To conclude their assessments of the heuristics, experts provided their opinions on the completeness of the set and could also suggest additional information that should have been considered. There were mixed views about the completeness of the thirteen heuristics for USec. An InfoSec expert and the HCI expert agreed that the set was complete while second InfoSec expert was undecided, and the USec expert disagreed that the set is complete. None of the experts suggested any additional information that should have been considered.

The USec expert stated that the applicability of the heuristics depends on who the user is. In a case where the user is an actual "genuine" user of the system, then all the heuristics are relevant. In a case where the user is an attacker, then all the heuristics may not be relevant because the system must now provide as little information as possible; hence the reason that USec is such a challenging field. In the real world, users cannot always be offered what they want owing to security concerns. The expert also stated that the views which are provided, reflect the notion that the user is an actual “genuine” user of the system and not an attacker.

The deductions from the heuristic assessments are that there are areas for possible improvements. Based on the results and comments, these include the following:

- Eliminate the convey features/expressiveness heuristic from the final USec HE.
- Consider the elimination of the identity signal heuristic from the final USec HE.
- Review the wording used in the descriptions of the revocability, aesthetics and minimalist design, errors, identity signal and security and privacy high-level heuristics.

7.2.4 Sheet IV – Checklist Items Assessment

The purpose of this sheet was to assess the checklist items for each high-level USec heuristic that was presented in section 7.2.3. These items were categorised under a high-level heuristic in phase 1 of the process for developing heuristics for SADs. Creating the checklist items by applying the tailored made method, grouping them and then reviewing their grouping as a whole are the outcomes of tasks 3, 4 and 5 respectively in phase 1.

The assessments specifically addressed the clarity, grouping and relevance of each checklist item. Experts also gave a final verdict for the item. As with the previous sheet, experts could provide optional comments to support their ratings. To conclude their assessments, experts provided their opinions on the completeness of the set of checklist items and could also suggest additional information that should have been considered. The aim was to gain consensus among the experts to ensure that the fields of HCI, InfoSec and USec are considered and represented. This can be challenging at times because the fields can offer conflicting views.

Measuring the clarity of the wording used for the checklist item would determine whether the terminology is clear and easy to understand or if re-wording is required in the next iteration cycle of the process. Measuring the grouping for a checklist item would determine if it is well categorised under a high-level heuristic. Measuring the relevance of a checklist item would determine whether it is appropriate in identifying a security/privacy usability violation. The verdict allows the expert to provide a final decision on whether or not the checklist item should be included in the USec HE. The number of checklist items included in each high-level heuristic is presented in table 7.4.

Table 7.4: The number of checklist items within each USec high-level heuristic

#	**Heuristic**	**Checklist Items**	**Numbering Order**
1	Visibility	4	1.1–1.4
2	Revocability	6	2.1–2.6
3	Clarity	4	3.1–3.4
4	Convey Features/Expressiveness	4	4.1–4.4
5	Learnability	7	5.1–5.7
6	Aesthetics and Minimalist Design	4	6.1–6.4
7	Errors	5	7.1–7.5
8	Satisfaction	3	8.1–8.3
9	User Suitability	6	9.1–9.6
10	User Language	6	10.1–10.6
11	User Assistance	5	11.1–11.5
13	Security and Privacy	27	13.1–13.27
12	Identity Signal	5	12.1–12.5

To measure the clarity, experts selected one of the following ratings: Very Good; Good; Barely Acceptable; Poor; or Very Poor, while they selected one of the following ratings: Strongly Agree; Agree; Undecided; Disagree or Strongly Disagree to assess grouping. To measure the relevance, experts used one of the following ratings: Very Relevant; Relevant; Moderately Relevant; Of Little Relevance or Not Relevant, and the ratings for their verdict included: Retain; Undecided or Remove. Each checklist item was evaluated on the basis for the aforementioned criteria. The checklist items that will be discussed in their particular sections based on the heuristics in which they are categorised, are those that did not receive any of the following ratings:

- Very Good/Good rating for their clarity
- Strongly Agree/Agree rating for their grouping
- Very Relevant/Relevant rating for their relevance
- Retain rating for their verdict

7.2.4.1 Visibility

Checklist item 1.2 states: *If pop-up windows are used to display security-related error messages, do they allow the user to see the field in error?* The item received a *Barely Acceptable* rating for its clarity and an *Undecided* verdict for keeping it in the USec HE. Both ratings were awarded by the USec expert. This expert noted that users tend to ignore pop-up windows. Hence, instead of pop-up windows a focus on messages that are displayed next to the field in question is preferred. The checklist item will be rephrased to represent this view.

To rate the completeness of the visibility checklist items, experts selected one of the following ratings: Yes; Not Sure and No. The results included one *Yes*, one *No* and two *Not Sure* ratings. A final comment from the USec expert is that visibility should also involve the security status information of a user. An InfoSec expert also commented on whether security actions should be visible before the user even initiates security operations. Both comments would be considered to improve the set of checklist items for visibility.

7.2.4.2 Revocability

Checklist item 2.1 states: *Do security options in menus make obvious whether de-selection is possible?* The item received a *Not Relevant* rating for its relevance and a *Remove* verdict. Both ratings were awarded by the USec expert. All the other experts rated the item as *Very Relevant* and *Retain*. Based on the overall ratings, the checklist item would not be modified and it would remain in the Revocability heuristic.

Checklist item 2.2 states: *Can users easily reverse their security actions?* The item received a *Barely Acceptable* rating for its clarity, a *Not Relevant* rating for its relevance and a *Remove* verdict. All ratings were awarded by the USec expert. All other experts rated the item as *Very Relevant* and *Retain*. The USec expert mentioned that the item needs to be rephrased because it is not feasible to easily reverse all security actions. The checklist item would be rephrased to represent this view and would remain in the Revocability heuristic.

Checklist item 2.5 states: *Can users cancel out of security operations in progress?* It received two *Undecided* ratings for its grouping, a *Moderately Relevant* rating for its relevance and an *Undecided* verdict. All ratings were awarded by the USec expert. The second grouping rating was awarded by the HCI expert. Interrupting a security action in progress is not important if users can still reverse it after the action is completed. Additionally, reversing security actions is considered in checklist item 2.2. Therefore, the checklist item would be eliminated from the Revocability heuristic.

Checklist item 2.6 states: *Is there an "undo" function at the level of a single security action or for a complete group of security actions?* It received a *Barely Acceptable* rating for its clarity, a *Disagree* rating for its grouping, a *Not Relevant* rating for its relevance and a *Remove* verdict. All ratings were awarded by the USec expert. Similar to checklist item 2.5, this has been considered in checklist item 2.2. Reducing the length of the USec HE is expressed in the results of the satisfaction questionnaires (see section 7.2.7). Since the checklist item is already covered in checklist item 2.2, it would be eliminated from the Revocability heuristic.

The ratings for the completeness of the revocability checklist items included three *Yes* ratings, while one expert did not provide a rating. No final comments were made by any of the experts.

7.2.4.3 Clarity

Checklist item 3.1 states: *Are users prompt to confirm security actions that have drastic, destructive consequences?* It received a *Moderately Relevant* rating for its relevance and a *Remove* verdict. The ratings were awarded by the USec expert. The expert explains that users ignore prompts and the best method in which to present prompts to users is yet to be determined. Despite this, it is still required for users to confirm a security action, which may have consequences for their own security. This is supported by the other experts, whom all rated the item as *Very Relevant*. The checklist item would not be modified and it would remain in the Clarity heuristic.

Checklist item 3.2 states: *Are the function keys that can cause the most serious consequences in hard-to-reach positions?* It received a *Strongly Disagree* rating for its grouping, a *Not Relevant* rating for its relevance and a *Remove* verdict from the USec expert. The HCI expert delivered an *Undecided* verdict. The ratings are supported by the perception that most security related actions are not achieved through function keys. The results showed that only the InfoSec experts agreed to keep the item. There was no consensus with the experts from the USec and HCI fields; therefore the checklist item would be eliminated from the Clarity heuristic.

Checklist item 3.3 states: *Does the system warn users if they are about to make a potentially serious security error?* Checklist item 3.4 states: *Does the system prevent users from making security errors whenever possible?* They both received *Poor* ratings by the USec expert for their clarity. Providing an example of the type of security errors for each item would assist evaluators to better understand their application. An example would be provided for each checklist item and they would remain in the Clarity heuristic.

The ratings for the completeness of the clarity checklist items included three *Not Sure* ratings, and one *Yes* rating. A final comment from the USec expert is that security error examples for items 3.3 and 3.4 should be provided. A comment form an InfoSec expert is that the system should also clearly explain why a specific security action should be taken (from a security viewpoint) and what are the risks for the user, if the action is not taken. Both comments would be considered to improve the set of checklist items for Clarity.

7.2.4.4 Convey Features/Expressiveness

The Convey features/expressiveness heuristic will be eliminated from the USec HE, as was discussed in section 7.2.3. However, the checklist that produced low scores will be mentioned.

Checklist item 4.1 states: *Are users' initiators of security actions rather than respondents?* The USec expert awarded the following scores; *Barely Acceptable* for the clarity, *Strongly Disagree* for the grouping, *Not Relevant* for the relevance and a *Remove* verdict. The ratings are supported by the view that the system always initiates security actions and not vice versa. The other experts were satisfied with the grouping of the item and no comments were made with regard to re-grouping it into another heuristic. Considering the USec expert's comments in combination with the elimination of the convey Features/expressiveness heuristic, the checklist item would also be eliminated.

Checklist item 4.2 states: *Does the system correctly anticipate and prompt for the users' probable next security-related activity?* The USec expert awarded a *Barely Acceptable* rating for the clarity. The other experts were satisfied with the grouping and no comments were made about re-grouping it into another heuristic. Considering this, in combination with the elimination of the convey Features/expressiveness heuristic, it was decided that the checklist item would also be eliminated.

Checklist item 4.3 states: *By looking, can the user tell the security state of the system, and the alternatives for security-related actions, if needed?* The USec expert awarded a *Strongly Disagree* rating for the grouping. The checklist item did receive *Very Relevant* ratings from the other experts, while the USec expert stated that the item is better located in the visibility heuristic. The one InfoSec expert also supported this view. Both views relate to a previous comment of the second InfoSec expert. The comment was made in the visibility checklist items, regarding the visibility of security actions before the user even initiates security operations. Taking these considerations into account, checklist item 4.3 would be re-grouped and categorised in the Visibility heuristic.

Checklist item 4.4 states: *Is there a clear understanding of the systems security capabilities?* Experts were satisfied with the grouping and no comments were made with regard to re-grouping it into another heuristic. Considering this in combination with the elimination of the convey Features/expressiveness heuristic, the checklist item would also be eliminated.

The ratings for the completeness of the Convey features/expressiveness checklist items included three *Yes* ratings, and one *Not Sure* rating. A comment form an InfoSec expert is whether the security capability claims of a system can be verified. This is an area for future research but beyond the scope of this work, even though it can impact on USec. Verifying that the security capabilities are maintained and adhered to would positively influence trust from the user perspective.

7.2.4.5 Learnability

Checklist item 5.1 states: *Have security items been grouped into logical zones, and have headings been used to distinguish between the zones?* The USec expert commented that there was uncertainty in the meaning of the item. All other experts rated its clarity as *Very Good*. Hence, the checklist item would not be modified and would remain in the Learnability heuristic.

Checklist item 5.3 states: *Are security operations easy to learn and use?* The USec expert suggests separating the item, as each; easy to learn and easy to use are fields of their own. The checklist item would be separated to represent this view and both items would remain in the Learnability heuristic.

Checklist item 5.4 states: *Are there security selection defaults?* The USec expert questions if this is desirable for security because users seldom change default settings and this could contribute to insecure behaviours. This is a valid point, yet two experts rated its relevance as *Very Relevant* and one as *Relevant*. It may be that it is beneficial to have default settings, nevertheless users must be made aware of their current default settings when interacting with the system for the first time. Oppositely, security is usually a secondary goal for users and it is likely that they will discard this type of information when it is presented to them. Nonetheless, the checklist item would be rephrased to represent this view and remain in the Learnability heuristic.

Checklist item 5.6 states: *Does the system protect users from making severe errors?* The item received a *Remove* verdict from the USec expert. The rating may relate to the fact that a system does not comply with this, has failed in its main objective, which is to protect the intended users. The two InfoSec experts rated its relevance as *Very Relevant* and the HCI expert as *Relevant*. Based on the overall scores, the checklist item would not be modified and it would remain in the Learnability heuristic.

Checklist item 5.7 states: *Is security-related information presented in a standardised manner?* An InfoSec expert commented that standardisation can be split between an individual system and across security systems. Users who interact with different security systems would require standardised terms across them. It is important to clarify that the USec HE does not only assess security systems. Moreover, it evaluates the security components of all applications/websites. In the case of the checklist item, it focuses on the individual system. It is unlikely for the security-related information of all systems to be presented in the same manner. The checklist item would be rephrased to represent the view that within the individual system, security-related information must be presented in a standardised manner. The item would remain in the Learnability heuristic.

The ratings for the completeness of the Learnability checklist items included two *Yes* ratings, while two experts did not provide a rating. The comments would be considered to improve the set of checklist items for Learnability.

7.2.4.6 Aesthetics and Minimalist Design

Checklist item 6.1 states: *Is only the security information essential to decision making displayed on the screen?* The USec expert commented that the item should address the user specifically. That is a valid point because it eliminates a possible misunderstanding; that of making essential security information viewable to an attacker. The checklist item would be rephrased to represent this view and it would remain in the Aesthetic and minimalist design heuristic.

Checklist item 6.4 states: *Are security prompts expressed in the affirmative?* The HCI expert awarded a *Barely Acceptable* rating for clarity, a *Moderately Relevant* rating for relevance and an *Undecided* verdict. Additional comments were not made, although the other experts' ratings support the inclusion of the item. An example would be provided to improve the item's clarity and it would remain in the Aesthetic and minimalist design heuristic.

The ratings for the completeness of the Aesthetic and minimalist design checklist items included two *Yes* ratings, one *Not Sure* rating, while one expert did not provide a rating. The comments would be considered to improve the set of checklist items for Aesthetic and minimalist design.

7.2.4.7 Errors

Checklist item 7.5 states: *Are the security-related error messages accurate in their descriptions?* The USec expert provided a *Barely Acceptable* rating for the clarity due to scepticism regarding the possibility of being accurate without providing too much information to an attacker. The ratings of the other experts supported the inclusion of the item. This checklist item would not be modified and it would remain in the Errors heuristic.

The ratings for the completeness of the Errors checklist items included two *Yes* ratings, one *Not Sure*, while one expert did not provide a rating.

7.2.4.8 Satisfaction

Checklist item 8.1 states: *Is each individual security setting a member of a family of security options?* The HCI expert awarded a *Barely Acceptable* rating for the clarity, an *Undecided* rating for grouping, a *Moderately Relevant* rating for relevance and an *Undecided* verdict. The USec expert also commented that the item is difficult to understand; hence, the checklist item would be eliminated. More details are provided in this regard when the completeness of the Satisfaction checklist items is discussed.

Checklist item 8.2 states: *Has colour been used specifically to draw attention and indicate status changes for security-related actions and information?* The HCI expert awarded a *Barely Acceptable* rating for clarity, an *Undecided* rating for grouping, a *Moderately Relevant* rating for relevance and an *Undecided* verdict. The USec expert was concerned about colour being a clear indicator, as it would not accommodate colour blind users. Additionally, security status was mentioned previously for inclusion in the visibility heuristic. Therefore, the item would be addressed in terms of visibility and would be eliminated from the satisfaction heuristic.

Checklist item 8.3 states: *Do security-related prompts imply that the user is in control?* The HCI expert awarded a *Barely Acceptable* rating for clarity, an *Undecided* rating for grouping, a *Moderately Relevant* rating for relevance and an *Undecided* verdict. The USec expert stated that in reality the system is always in control with regard to security and users should not be misled by thinking otherwise. The checklist item would be eliminated and details will be provided when the completeness is discussed.

The ratings for the completeness of the satisfaction checklist items included one *Yes* rating, one *Not Sure* rating, one *No* rating, while one expert did not provide a rating. A final comment from the HCI expert was that all items did not seem to be focused on user satisfaction. Meanwhile, the USec expert queried whether it is even possible to satisfy users. It would seem that this is difficult to quantify and presents a new area of research. The purpose of the USec HE is to assist developers to design usable features for security and privacy. Ultimately, this will impact on the users' experiences. Hence, it is important that the checklist items can be used to assist in this quest by making their applicability and understanding possible. Checklist items 8.1 and 8.3 fail in this regard and, being a new area, they are difficult to quantify. Therefore they would be eliminated, while item 8.2 would be accommodated in the visibility heuristic.

In section 7.2.3, the importance of the satisfaction heuristic was measured as it achieved high scores and worthy support for its inclusion. It was also mentioned that the heuristic is essential and that it will be retained. Following the assessments of its checklist items, it has been established that it should instead be eliminated from the USec HE. This is due to the fact that items 8.1 and 8.3 have been eliminated and item 8.2 would be re-grouped in the visibility heuristic.

7.2.4.9 User Suitability

Checklist item 9.1 states: *If the system supports both novice and expert users, are multiple levels of security error messages detail available?* The USec expert delivered a *Remove* verdict, albeit making a supporting comment that tailoring error messages according to the expertise of users is an interesting concept. The ratings of the other experts strongly supported the inclusion of the item. Hence, this checklist item would not be modified and would remain in the User suitability heuristic.

Checklist item 9.3 states: *If the system supports both novice and expert users, are multiple levels of security detail available?* The USec expert delivered a *Remove* verdict, although the ratings of the other experts strongly supported the inclusion of the item. The checklist item would therefore not be modified and would remain in the User suitability heuristic.

Checklist item 9.4 states: *Can users easily change the level of security detail?* The USec expert delivered a *Remove* verdict, while the HCI expert awarded a *Barely Acceptable* rating for clarity, an *Undecided* rating for grouping, a *Moderately Relevant* rating for relevance and an *Undecided* verdict. However, both the InfoSec experts were satisfied with the item. Considering that there is no consensus with the HCI and USec experts, the checklist item would be eliminated from the User suitability heuristic.

Checklist item 9.5 states: *Can users easily change between novice and expert levels?* The USec expert delivered a *Remove* verdict. The HCI expert awarded a *Barely Acceptable* rating for clarity, an *Undecided* rating for grouping, a *Moderately Relevant* rating for relevance and an *Undecided* verdict. However, the InfoSec experts were yet again satisfied with the item. However, as with the previous item, there is no consensus between the three fields and therefore the checklist item would be eliminated from the User suitability heuristic.

The ratings for the completeness of the User suitability checklist items included one *Yes* rating, two *Not Sure* ratings, while one expert did not provide a rating. The comments would be considered to improve the set of checklist items for aesthetic and minimalist design. A comment from an InfoSec expert is that security help/training should also be tailored to the expertise of the user. This comment would be considered in the User assistance heuristic. The USec expert commented that the concept in this heuristic seems to be to tailor for the security expertise of the user. Although this is important for usability, there is a concern about its relevance within the security area.

7.2.4.10 User Language

All experts were pleased with the checklist items for the User language heuristic. The USec expert suggested examples for items 10.5 and 10.6: checklist item 10.5: *Is privacy jargon avoided?* Checklist item 10.6: *Is security jargon avoided?*

The ratings for the completeness of the User language checklist items included one *Yes* rating, two *Not Sure* ratings, while one expert did not provide a rating. An InfoSec expert probed whether the naming of checklist items 10.1 and 10.2 related directly to the security related role of an action. Examples would be provided to distinguish between the naming of security actions and objects in 10.1 and 10.2.

7.2.4.11 User Assistance

All experts were pleased with the checklist items for the User assistance heuristic. Previously, in the User suitability heuristic, an InfoSec expert mentioned that it would be useful to provide assistance that is tailored to user expertise (e.g. novice or expert). A checklist item would thus be provided to express this view and it would be included in the User assistance heuristic.

The ratings for the completeness of the User assistance checklist items included one *Yes* rating, two *Not Sure* ratings, while one expert did not provide a rating.

7.2.4.12 Identity Signal

Overall, experts awarded high ratings for the checklist items of the Identity signal heuristic. However, an InfoSec expert and the USec expert stressed that the type of information included in an identity signal will be beyond the security knowledge of a novice user. In addition, novice users do not usually read such information and are likely to interact with non-trustworthy sources, even though they are warned beforehand. The second InfoSec commented that it would be useful to have a feature in the identity signal for immediate verification of the Issuer, who provides the certificate. The experts understand the importance of the identity signal but are not convinced of its usefulness to novice users.

In section 7.2.3, the identity signal was mentioned as a heuristic for possible elimination. Based on the above comments, the idea is not to eliminate the Identity signal heuristic but rather to eliminate checklist items that seem to be too complex for novice users and to retain those that are more understandable. Checklist item 12.3 states: *Does the identity signal include human-readable information about the certificate subject?* Checklist item 12.4 states: *Does the identity signal include the Issuer fields' organisation attribute to inform the user about the party responsible for that information?* As a result, checklist items 12.3 and 12.4 will be eliminated from the identity signal heuristic.

Checklist item 12.5 states: *Are there privacy indicators informing users about the privacy practices of the system?* Experts were satisfied with this item, based on their ratings. However, after items 12.3 and 12.4 were eliminated, item 12.5 had to be regrouped. The improvements made to the aesthetic and minimalist design heuristic contributed to this decision. Item 12.5 is now better represented in this heuristic because it relates to visual design. Retaining the item in the USec HE is well supported because it aids in protecting sensitive information that can be manipulated (e.g. OHSN, E-learning etc.).

The ratings for the completeness of the Identity signal checklist items included one *Yes* rating, two *Not Sure* ratings, while one expert did not provide a rating.

7.2.4.13 Security and Privacy

Checklist item 13.1 states: *Are protected areas completely inaccessible?* An InfoSec expert awarded a *Moderately Relevant* rating for relevance and an *Undecided* verdict. The expert also commented that certain areas would probably be read-only but not modifiable. The USec expert delivered a *Remove* verdict and commented that this is not a usability issue and therefore should not be considered as a USec violation. The checklist item would be eliminated from the Security and privacy heuristic.

Checklist item 13.2 states: *Can protected or confidential areas be accessed with certain passwords?* An InfoSec expert and the USec expert suggested that the term *passwords* is too restrictive because it only represents a single form of authentication. The checklist item would be rephrased and would remain in the Security and privacy heuristic.

Checklist item 13.5 states: *Does the system grant access to a user based on valid authorization?* The USec expert commentated that this is not a usability issue; instead, it is a requirement for the system to function correctly. Hence, the item should not be considered as a USec violation. The checklist item would accordingly be eliminated from the Security and privacy heuristic.

Checklist item 13.7 states: *In the case where the user must provide sensitive personal information, does the system state what measures are used to protect this data?* The USec expert commented that the system should also ensure that those measures are actually taken. Hence the checklist item would be rephrased and would remain in the Security and privacy heuristic.

Checklist items 13.8 and 13.9 respectively state: *Does the system notify users on their access privileges? Does the system initiate a session lock after a period of inactivity or upon user request?* Based on the experts' previous comments, these items are examples for showing a user's security status. Accordingly a checklist item has been included in the visibility heuristic to address this. As a result items 13.8 and 13.9 will be eliminated from the Security and privacy heuristic.

Checklist item 13.11 states: *Are notification messages relating to security and privacy displayed to the user before access to the system is granted?* The USec expert delivered a *Remove* verdict by arguing that users will not read the messages because they are goal directed to their main activity. Nonetheless, the other experts awarded high scores for this item. Consequently, it would not be modified and it would remain in the Security and privacy heuristic.

Checklist item 13.14 states: *Does the system install required software updates automatically and notify the user about this action?* The USec expert delivered a *Remove* verdict by arguing that this can be regarded as a security violation since it is an action not prompted by the user. Additionally, an InfoSec expert awarded an *Undecided* rating for the grouping and did not provide additional comments. Based on the ratings and concerns, the item would be eliminated from the Security and privacy heuristic.

Checklist item 13.15 states: *Does the system employ automated tools that provide notification to the user upon discovering discrepancies during integrity verification?* The USec expert delivered an *Undecided* verdict on the basis that this will be useful only if the users know what to do about it. Nonetheless, the other experts awarded high scores for this item. Consequently, it would not be modified and it would remain in the Security and privacy heuristic.

Checklist item 13.18 states: *Does the system notify the user of any information system weaknesses or vulnerabilities associated with reported security incidents?* The USec expert delivered a *Remove* verdict on the basis that this is more of a legality issue, and although it affects the user, it is beyond the scope of USec. Nonetheless, the other experts awarded high scores for this item. Consequently, it would not be modified and it would remain in the Security and privacy heuristic.

Checklist item 13.19 states: *Does the system notify the user about the conduct of backups relating to their personal information?* The USec expert delivered a *Remove* verdict on the basis that this is not usually done in practice and that the average user would not be interested either. However, it would be better to instead provide a contact for any security-related questions users may have. In addition, the other experts awarded high scores for this item.

Taking all into account, the checklist item would be rephrased and would remain in the Security and privacy heuristic.

Checklist item 13.20 states: *Is there a backup policy that regulates how copies of information should be taken and tested regularly?* An InfoSec expert awarded an *Undecided* rating for the grouping and argued whether backups could be considered specific to privacy. The other experts awarded high scores for this item. Consequently, it would not be modified and it would remain in the Security and privacy heuristic.

Checklist item 13.21 states: *Does the system provide awareness and educate the user on how to complete tasks?* An InfoSec expert awarded an *Undecided* rating for the grouping and the USec expert delivered a *Remove* verdict. The InfoSec expert was not convinced that awareness relates to privacy while the USec expert maintained that since security is not the users' main goal; there is no need to provide awareness for completing security tasks. Based on the ratings and concerns, the item would be eliminated from the Security and privacy heuristic.

Checklist item 13.22 states: *Does the system enforce minimum password complexity of defined requirements?* The USec expert delivered a *Remove* verdict. The expert added that passwords are a research area in their own right and that there is no agreement on password strength or indeed whether such restrictions do more good than harm. Nonetheless, the other experts awarded high scores for this item. Consequently, it would not be modified and it would remain in the Security and privacy heuristic.

Checklist item 13.24 states: *Does the system enforce password minimum and maximum lifetime restrictions?* An InfoSec expert awarded an *Undecided* rating for grouping and a *Moderately Relevant* rating for relevance and delivered an *Undecided* verdict. The USec expert delivered a *Remove* verdict. Both experts agreed that this can in fact negatively affect security. The USec expert mentions that changing passwords regularly can reduce security because users will write them down or choose increasingly weak ones. In line with this view, the InfoSec expert mentions that forcing too complex passwords, or too many changes, or preventing password reuse, all lead to users writing passwords down. Based on the ratings and concerns, the item would be eliminated from the Security and privacy heuristic.

Checklist item 13.25 states: *Does the system prohibit password reuse for a defined number of generations?* An InfoSec expert awarded an *Undecided* rating for grouping, a *Moderately*

Relevant rating for relevance and an *Undecided* verdict. No additional comments were made. Yet, the ratings are likely to be based on the comments the same expert made in terms of item 13.24. However, the other experts awarded high scores for this item. Consequently it would not be modified and it would remain in the Security and privacy heuristic.

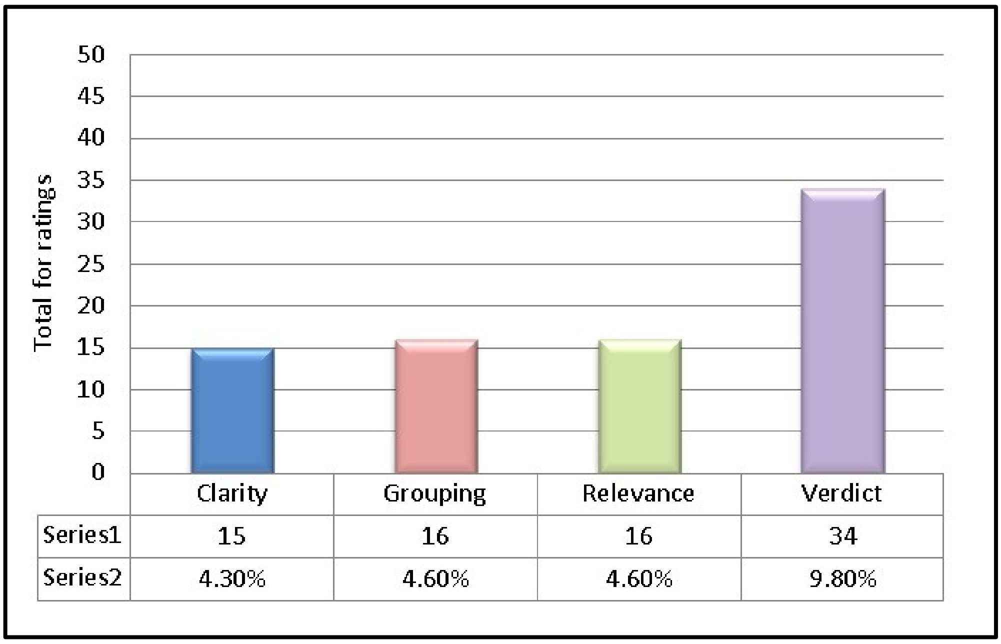
Checklist item 13.27 states: *Does the system require users to confirm statements indicating that they understand the conditions of access?* The USec expert suggested providing an example. Thus, an example would be included with the checklist item and it would remain in the Security and privacy heuristic.

The ratings for the completeness of the Security and privacy checklist items included two *Yes* ratings, one *Not Sure* rating, while one expert did not provide a rating. Final comments were made by an InfoSec expert. This expert queried whether users should be able to select and ultimately provide consent for what personal information can be used and how it is used, as this should not just be a common accept-or-deny situation that covers all information. This is an interesting idea that requires further investigation. Checklist item 13.27 addresses this to a small extent and the manner in which privacy policies/statements are presented online is a well-studied area. Once again, this can impact on USec, but such a discussion is beyond the scope of the USec He. The purpose here was to assess the checklist items, which were developed by conducting a literature review in phase 1 and determining the most usable manner in which to present privacy policies to users was not an integral part of the literature review. Additionally, the InfoSec expert suggests that security and privacy statements must be concise. A checklist item would thus be included to address this suggestion.

In review, there were a total of four experts who evaluated 86 checklist items for clarity, grouping, relevance and verdict. This provides a total of three hundred and forty-four possible responses, which represent their ratings. The graph in figure 7.3 displays the number of low ratings awarded for each of the criteria, which is the sum of low ratings from all experts. Series 1 represents the actual number of low ratings from the three hundred and forty-four in total; and series 2 represents the low rating percentage for the particular criterion. In terms of figure 7.3, low ratings are defined as the checklist items that did not receive any of the following ratings:

- Very Good/Good rating for their clarity
- Strongly Agree/Agree rating for their grouping
- Very Relevant/Relevant rating for their relevance

- Retain rating for their verdict



	Clarity	Grouping	Relevance	Verdict
Series1	15	16	16	34
Series2	4.30%	4.60%	4.60%	9.80%

Figure 7.3: Low ratings for checklist items based the criteria

The deductions from the checklist item assessments, based on the results and comments of the experts, are

- Eliminate the convey features/expressiveness and satisfaction heuristics.
- Retain the identity signal heuristic.
- Eliminate checklist items 2.5 and 2.6 from the revocability heuristic.
- Eliminate checklist item 3.2 from the clarity heuristic.
- Add a new checklist item in the clarity heuristic that explains why security actions must be taken and the consequences of not taking them.
- Eliminate checklist items 4.1, 4.2 and 4.4 from the convey features/expressiveness heuristic.
- Re-group checklist item 4.3 and categorise it in the visibility heuristic.
- Eliminate checklist items 8.1 and 8.3 from the satisfaction heuristic.
- Address checklist item 8.2 in the visibility heuristic and eliminate it from the satisfaction heuristic.
- Eliminate checklist items 9.4 and 9.5 from the user suitability heuristic.
- Add a new checklist item to the user assistance heuristic that focuses on providing security help according to the level of user expertise.
- Eliminate checklist items 12.3 and 12.4 from the identity signal heuristic.

- Re-group checklist item 12.5 and categorise it in the aesthetics and minimalist design heuristic.
- Eliminate checklist items 13.1, 13.5, 13.14, 13.21 and 13.24 from the security and privacy heuristic.
- Address checklist items 13.8 and 13.9 in the visibility heuristic and eliminate them from the security and privacy heuristic.
- Add a new checklist item in the security and privacy heuristic that focuses on providing concise security and privacy statements.
- Provide examples for checklist items 2.4, 3.2, 3.3, 6.4, 10.1, 10.2, 10.5, 10.6 and 13.27.
- Rephrase the checklist items 1.2, 2.2, 5.4, 5.7, 6.1, 13.2, 13.7 and 13.19.
- Separate checklist item 5.3.

The above deductions will be addressed and the improved USec HE will be presented in chapter 8. In table 6.10, the issues that participants had with checklist items were presented. These were deduced from the application of the USec HE when evaluating the two OHSNs. Their concerns will also be considered in the improved USec HE. Table 7.5 presents the checklist items that participants expressed concerns about as well as the problem is also presented. The table shows whether the experts shared the same view with a participant for a specific problem and lastly presents the outcome of the problem.

Table 7.5: Addressing the participant issues with the checklist items

Checklist Item	**Problem**	**Expert Agreement**	**Outcome**
1.2	Rephrase suggested	√	Item has been rephrased
4.1	Rephrase suggested	X	Item has been eliminated due to expert ratings/comments
5.1	Disagree with grouping	X	Item remains in original group since all experts were satisfied
6.1	Rephrase suggested	√	Item has been rephrased
6.4	Example suggested	√	Example included
8.3	Examples suggested	X	Item has been eliminated however due to expert ratings/comments
11.3	Rephrase suggested	X	Item has been rephrased
11.4	Relevance of item depends on situation	X	Item remains unchanged since all experts were satisfied

Checklist Item	Problem	Expert Agreement	Outcome
11.5	Rephrase suggested	X	Item has been rephrased
13.2	Rephrase suggested	√	Item has been rephrased
13.11	Rephrase suggested	X	Example included
13.15	Rephrase suggested	X	Item has been rephrased

7.2.5 Sheet V – Severity Ratings

Severity ratings are applied to measure the extent of usability violations in an HE. Jakob Nielsen awarded his own severity ratings in combination with his well-known usability heuristic set. Although they have been widely adopted for HEs, there are cases where they are insufficient to measure the extent of usability violations in a SAD, as was determined by Sim et al. (2009) when they created heuristics to evaluate computer assisted assessment applications. The same rationale exists in this study with regard to the severity ratings for the USec HE, as there was a need to create customised severity ratings that can be more effective in measuring the extent of USec violations. This is because Nielsen's severity ratings are based solely on a usability perspective, and consequently, they lack a security perspective. Taking into account Nielsen's severity ratings (Nielsen, 1994), and by modifying and adapting them with the standards for security categorisation of federal information and information systems (FIPS PUB 199, 2004), it was possible to include a security perspective in them as well to compliment a usability one. The result was two different sets of USec severity ratings that experts would assess in order to determine the most effective match for the USec HE.

Nielsen used a four-level rating scale to measure the severity of usability problems. Experts will evaluate the interface and if they determine a usability violation, they will rate it with a value of 0 – 4 in order to measure its extent. The ratings include:

0. I don't agree that this is a usability problem at all.
1. Cosmetic problem only: need not be fixed unless extra time is available on project.
2. Minor usability problem: fixing this should be given low priority.
3. Major usability problem: important to fix, so should be given high priority.
4. Usability catastrophe: imperative to fix this before product can be released.

Investigating the potential impact of a security breach for organisations and individuals provided a potential platform to integrate security with Nielsen's severity ratings. FIPS Publication 199 defines three levels of potential impact on organisations or individuals should there be a breach of security (i.e. a loss of confidentiality, integrity, or availability). The application of these definitions must take place within the context of each organisation and the overall national interest. The three levels of impact are defined and include (FIPS PUB 199, 2004):

1. The potential impact is *LOW* if the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organisational operations, organisational assets, or individuals.
2. The potential impact is *MODERATE* if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organisational operations, organisational assets, or individuals.
3. The potential impact is *HIGH* if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organisational operations, organisational assets, or individuals.

Nielsen's severity ratings and FIPS three levels of potential impact of a security breach helped determine two sets of USec severity ratings. It is important that severity ratings are easy to understand and apply to a violation in a manner that makes the extent of the violation comprehensible. By considering all these factors, two USec severity rating sets were presented. Set 1 is presented in table 7.6.

Table 7.6: USec severity ratings for Set 1

Rating	Severity classification
0	I do not agree that this is a USec violation at all.
1	Minor USec violation: the potential impact is *LOW* therefore fixing this should be given a low priority.
2	Modest USec violation: the potential impact is *MODERATE* therefore fixing this should be given a moderate priority.
3	Major USec violation: the potential impact is *HIGH* therefore it is important to fix and should be given a high priority.
4	USec catastrophe: the potential impact is *SEVERE* and therefore it is imperative to fix before product can be released.

Accompanying the USec severity ratings for Set 1 were the following potential impact descriptions:

- *LOW* potential impact: security/privacy is maintained and usability is at an acceptable level
- *MODERATE* potential impact: security/privacy is maintained and usability is not at a reasonable level
- *HIGH* potential impact: security/privacy is not maintained and usability is at a satisfactory level
- *SEVERE* potential impact: security/privacy and usability is not maintained

The potential impacts are more serious when security and privacy are not maintained in comparison to usability. In the context of online social networking environments, where users' personal information is constantly at risk, protection is key. The USec severity ratings must also determine if the violation occurs because it fails from a security or usability standpoint. This is demonstrated in the construction of both sets – Set 2 follows the same logic as Set 1, although it does represent a simpler version of it. Set 2 is presented in table 7.7.

Table 7.7: USec severity ratings for Set 2

Rating	Severity Classification
0	Secure and usable
1	Secure and moderately usable
2	Secure and not usable
3	Not secure and usable
4	Not secure and not usable

The expert assessment examined the severity ratings for Sets 1 and 2 separately. It specifically addressed the ease of application and relevance of each set. Experts could also provide optional comments were they felt necessary, although one of the four experts did not complete this sheet. Tables 7.8 and 7.9 summarise the frequencies of the experts' responses (n = 3) for the ease of application and relevance of Set 1. In table 7.8 the scores are representative of the number of experts that selected the following: VE = Very Easy; E = Easy; U = Undecided; D = Difficult and VD = Very Difficult.

Table 7.8: Overall ratings for the ease of application of the USec severity ratings for Set 1

Rating	Severity classification	VE	E	U	D	VD
0	I do not agree that this is a USec violation at all	2			1	
1	Minor USec violation: the potential impact is *LOW* therefore fixing this should be given a low priority	2			1	
2	Modest USec violation: the potential impact is *MODERATE* therefore fixing this should be given a moderate priority	2	1			

Rating	Severity classification	VE	E	U	D	VD
3	Major USec violation: The potential impact is *HIGH* therefore it is important to fix and should be given a high priority	2	1			
4	USec catastrophe: The potential impact is *SEVERE* and therefore it is imperative to fix before product can be released	2	1			

The results show that the severity ratings in Set 1 are in general easy to apply when evaluating an interface for USec violations. However, an expert in the InfoSec field stated that ratings 0 and 1 were difficult to apply. The expert did not provide additional comments to further explain these views. However, according to their results, the other two experts, from InfoSec and HCI fields were satisfied with the ease of application. Table 7.9 focuses on the relevance of the severity ratings. All experts rated each of the severity ratings as very relevant for measuring USec violations. In table 7.9 the scores are representative of the number of experts that selected the following: VR = Very Relevant; R = Relevant; MR = Moderately Relevant; OLR = Of Little Relevance and NR = Not Relevant.

Table 7.9: Overall ratings for the relevance of the USec severity ratings for Set 1

Rating	Severity Classification	VR	R	MR	OLR	NR
0	I do not agree that this is a USec violation at all.	3				
1	Minor USec violation: the potential impact is *LOW* therefore fixing this should be given a low priority.	3				
2	Modest USec violation: the potential impact is *MODERATE* therefore fixing this should be given a moderate priority.	3				
3	Major USec violation: The potential impact is *HIGH* therefore it is important to fix and should be given a high priority.	3				
4	USec catastrophe: The potential impact is *SEVERE* and therefore it is imperative to fix before product can be released.	3				

Tables 7.10 and 7.11 summarise the frequencies of the experts' responses (n = 3) for the ease of application and relevance of Set 2 respectively. In table 7.10, the scores are representative of the number of experts that selected the following: VE = Very Easy; E = Easy; U = Undecided; D = Difficult and VD = Very Difficult.

Table 7.10: Overall ratings for the ease of application of the USec severity ratings for Set 2

Rating	Severity classification	VE	E	U	D	VD
0	Secure and usable	2				1
1	Secure and moderately usable	1	1		1	
2	Secure and not usable	2	1			
3	Not secure and usable	2	1			
4	Not secure and not usable	3				

The results for the ease of application of Set 2 are similar to those from Set 1. The InfoSec expert, who scored severity ratings 0 and 1 as *Difficult* in Set 1, rated them as *Very Difficult* and *Difficult* in Set 2. More concerning is the score assigned to severity rating 1, as it may require revision. Regarding severity rating 0, it is common practice to include such a rating and HCI experts will be well aware of the use and application. Hence, it may be the background of the specific expert that influenced the scores awarded it because it might not make sense to have a severity rating for a feature that does not classify as a violation.

The second InfoSec expert scored severity ratings 2 and 3 as *Easy*. From the additional comments provided it can be established that improving the wording of the specific severity ratings could have resulted in *Very Easy* scores for both. In particular, the expert would have preferred the severity classification to be *Secure but not usable* for severity rating 2 and *Usable but not secure* for severity rating 3. Overall, the results indicate that the severity ratings in Set 2 can also be considered as easy to apply, when evaluating an interface for USec violations.

Table 7.11 focuses on the relevance of the severity ratings for Set 2. Once again, the results mimic those of Set 1. All experts rated each of the severity rating as very relevant for measuring USec violations. In table 7.11 the scores are representative of the number of experts that selected the following: VR = Very Relevant; R = Relevant; MR = Moderately Relevant; OLR = Of Little Relevance and NR = Not Relevant.

Table 7.11: Overall ratings for the relevance of the USec severity ratings for Set 2

Rating	Severity Classification	VR	R	MR	OLR	NR
0	Secure and usable	3				
1	Secure and moderately usable	3				
2	Secure and not usable	3				
3	Not secure and usable	3				
4	Not secure and not usable	3				

To conclude their assessments of the severity ratings, experts gave their opinions regarding the completeness of each set and could also suggest additional information that should have been considered. They then selected the USec severity rating set that they preferred. All experts expressed the opinion that both sets are complete and, therefore, did not suggest any additional information that should have been considered. Set 1 was the preferred set of the two, being preferred by two experts, one from HCI and one from InfoSec. The other InfoSec expert preferred Set 2.

The deductions from the severity ratings assessments are that the USec severity ratings of Set 1 represent the preferred option when measuring the extent of USec violations on an interface. These are easy to apply and are very relevant for their purpose. Areas for possible improvements that have been suggested include the following:

- Review wording for severity rating 0 of Set 1
- Review wording for severity rating 1 of Set 1

7.2.6 Sheet VI – Material Assessment

The focus of this sheet was to assess the material that was considered to develop the USec HE. The assessment examined the usability and USec material and the security and privacy material separately and specifically addressed the novelty and relevance of the materials. Experts could also provide optional comments were they felt necessary, but one of the four experts did not complete this sheet. Tables 7.12 and 7.13 summarise the frequencies of the experts' responses (n = 3) for the novelty and relevance of the usability and USec material respectively. In table 7.12 the scores are representative of the number of experts that selected the following: UTD = Up To Date; PU = Partially Updated; OD = Out Dated; and NDE = Not Domain Expert.

Table 7.12: Overall ratings for the novelty of usability and USec material

#	Document	UTD	PU	OD	NDE
1	Web security context: UI guidelines	3			
2	10 principles for secure interaction design	2	1		
3	6 criteria for HCI-S	2	1		
4	10 preliminary guidelines for USec	2	1		
5	Xerox HE checklist	1	1		1

The results from table 7.12 are positive and show a consensus among the experts. Their general view is that none of the usability and USec material is outdated. All experts rated the Web security context UI guidelines as *Up to Date*. Two experts rated the ten principles for secure interaction design as *Up to Date* and one as *Partially Updated*. Similarly, two experts rated the six criteria for HCI-S as *Up to Date* and one as *Partially Updated*. The same ratings were provided for the 10 preliminary guidelines for USec with two *Up to Date* and one *Partially Updated*. Finally, the Xerox HE checklist gave mixed scores; one *Up to Date* one *Partially Updated* and one *Not Domain Expert*.

Table 7.13 focuses on the relevance of the material for usability and USec. In table 7.13 the scores are representative of the number of experts that selected the following: VR = Very Relevant; R = Relevant; MR = Moderately Relevant; OLR = Of Little Relevance; NR = Not Relevant; and NDE = Not Domain Expert.

Table 7.13: Overall ratings for the relevance of usability and USec material

#	Document	VR	R	MR	OLR	NR	NDE
1	Web security context: user interface guidelines	3					
2	10 principles for secure interaction design	3					
3	6 criteria for HCI-S	3					
4	10 preliminary guidelines for USec	2	1				
5	Xerox HE checklist	3					

The results from table 7.13 again show a consensus among the experts. Their general view is that the usability and USec material considered are very relevant. All experts rated the Web security context UI guidelines and the ten principles for secure interaction design as *Very Relevant*; similarly, all three rated the six criteria for HCI-S as *Very Relevant*. Two experts rated the ten preliminary guidelines for USec as *Very Relevant* and one as *Relevant*. Finally, all experts once again rated the Xerox HE checklist as *Very Relevant*. This is particularly pleasing because the Xerox HE was the well-known heuristic set used for the tailored made method in order to develop the checklist items for the USec heuristics.

Tables 7.14 and 7.15 summarise the frequencies of the experts' responses (n = 3) for the novelty and relevance of the security and privacy material respectively. In table 7.14 the scores are representative of the number of experts that selected the following: UTD = Up To Date; PU = Partially Updated; OD = Out Dated; and NDE = Not Domain Expert.

Table 7.14: Overall ratings for the novelty of security and privacy material

#	Document	UTD	PU	OD	NDE
1	EU data protection regulations	1	1		1
2	Security-inherent properties combined with ISO 9241	2	1		
3	Privacy space framework	1	1		1
4	Privacy guidelines of Cranor	1	1		1
5	ISO/IEC 27002	2	1		
6	NIST Special Publication 800-53	1	1		1

The results from table 7.14 are respectable in that none of the experts rated any of the security and privacy material as outdated. One expert rated the EU data protection regulations as *Up to Date*, one as *Partially Updated* and one responded *Not Domain Expert*. Two experts rated the security-inherent properties combined with ISO 9241 as *Up to Date* and one as *Partially*

Updated. One expert rated the privacy space framework as *Up to Date*, one as *Partially Updated* and one answered *Not Domain Expert*. The same results were provided for the privacy guidelines of Cranor, with one *Up to Date*, one *Partially Updated* and one *Not Domain Expert*. Two experts rated ISO/IEC 27002 as *Up to Date* and one as *Partially Updated*. Finally, the NIST Special Publication 800-53 had mixed scores; one *Up to Date* one *Partially Updated* and one *Not Domain Expert*.

Table 7.15 focuses on the relevance of the material for security and privacy. In table 7.15 the scores are representative of the number of experts that selected the following: VR = Very Relevant; R = Relevant; MR = Moderately Relevant; OLR = Of Little Relevance; NR = Not Relevant; and NDE = Not Domain Expert.

Table 7.15: Overall ratings for the relevance of security and privacy material

#	Document	VR	R	MR	OLR	NR	NDE
1	EU data protection regulations	3					
2	Security-inherent properties combined with ISO 9241	2	1				
3	Privacy space framework	2	1				
4	Privacy guidelines of Cranor	1	2				
5	ISO/IEC 27002	3					
6	NIST Special Publication 800-53	2	1				

The results displayed in table 7.15 show a consensus among the experts. Their general view is that the security and privacy material considered is very relevant. This can be concluded because three of the five have been awarded *Relevant* scores by the HCI expert. With regards to the security and privacy material, the opinions of the InfoSec experts hold more value, as it is them who determine whether security and privacy have been well represented in the USec HE. All experts rated the EU data protection regulations as *Very Relevant*. Moreover, two experts rated the security-inherent properties combined with ISO 9241 as *Very Relevant* and one as *Relevant*. The same results were awarded for the privacy space framework, with two *Very Relevant* and one *Relevant*. One expert rated Cranor's privacy guidelines as *Very Relevant* and the other two as *Relevant*. All experts rated ISO/IEC 27002 as *Very Relevant*. Finally, two experts rated the NIST Special Publication 800-53 as *Very Relevant* and one as *Relevant*.

To complete their assessments of the materials, experts gave their overall opinions. Moreover, they were given an opportunity to suggest additional materials that should have been considered. All experts suggested that the usability and USec material was complete and none provided suggestions for additional material to be considered. In terms of the security and privacy material, two experts suggested it was complete, while one was not sure about completeness. However, that expert did not suggest alternative materials that could be considered, nor did the other two experts suggest additional materials.

The deductions from the material assessments are that the usability and USec material is not out dated and is particularly relevant. The same applies to the security and privacy materials. Accordingly, no areas for possible improvements were identified with regard to the materials of each field – InfoSec and HCI.

7.2.7 Sheet VII – User Satisfaction Questionnaire

The final sheet in the validation tool was a user satisfaction questionnaire. This was similar to the one answered by participants in the FUE in section 6.3.3, which was conducted on the OHSNs. However, this questionnaire contained more items, eighteen to be exact, and focused on the experts' views regarding the USec HE as a tool for assessing the level of USec in online social networking environments. Table 7.16 summarises the frequencies of the experts' responses (n = 3). It should be noted that one of the four experts did not complete this sheet in their validation and another did not answer question 14. In table 7.16 the scores for questions 1 to 13 are representative of the number of experts that selected the following: SA = Strongly Agree; A = Agree; U = Undecided; D = Disagree; and SD = Strongly Disagree.

The scores for question 14 are representative of the number of experts that selected the following: VI = Very Important; I = Important; MI = Moderately Important; OLI = Of Little Importance; and U = Unimportant.

The scores for questions 15 and 16 are representative of the number of experts that selected the following: VG = Very Good; G = Good; BA = Barely Acceptable; P = Poor; and VP = Very Poor.

Last of all, the scores for question 17 are representative of the number of experts that selected the following: VU = Very Useful; U = Useful; BU = Barely Useful; NU = Not Useful; and NVU = Not Very Useful. Following table 7.16 is an analysis of the questions and their relating scores.

Most of the questions that the participants had in the FUE, which are listed in table 6.12, were also provided to the experts. In particular, the first eleven questions are identical. However, questions 12, 13 and 17 in table 7.16 were only provided to the experts. Questions 15 and 16 in table 7.16 are identical to questions 13 and 14 respectively, in table 6.12.

Table 7.16: Overall ratings from user satisfaction questionnaire

#	Question	SA	A	U	D	SD
1	I can evaluate a security and privacy feature quickly applying the checklist items.	1	2			
2	I am satisfied with the number of checklist items included.		2		1	
3	The length of the USec HE should be shortened.	1	1	1		
4	It is easy to understand how to apply the USec HE on an interface.	2		1		
5	The heuristic descriptions clearly describe what the checklist items are evaluating.	1	2			
6	The terminology used in the USec HE is clear and easy to understand.	1	2			
7	I would need additional instructions to evaluate an interface with the USec HE.		1		2	
8	It is easy to learn how to use the USec HE once you have used it once.	2		1		
9	Checklist items are well categorised under a heuristic.	2		1		
10	The amount of information included in the USec HE was useful.	1	1	1		
11	The use of the USec HE is complex		1		2	
12	The proposed USec severity ratings are effective in measuring the degree of a security/privacy usability violation.		2	1		
13	The material used to develop the USec HE is acceptable and sufficient?	2	1			
#	**Question**	**VI**	**I**	**MI**	**OLI**	**U**
14	Developing tools that improve the usability of security and privacy features on an interface.		2			
#	**Question**	**VG**	**G**	**BA**	**P**	**VP**
15	Overall, how would you rate the quality of the USec HE?	2	1			
16	Overall, how would you rate the effectiveness of the USec HE?		3			
#	**Question**	**VU**	**U**	**BU**	**NU**	**NVU**
17	Overall, how useful is the USec HE to identify security/privacy usability violations on an interface?	2	1			

Question 1 examined the time required to evaluate security and privacy features on a website, using the USec HE. Two experts *Agree* and one *Strongly Agree* that the evaluation can be done quickly by applying the relevant checklist items. It is important that the tool can be used

quickly as this can contribute to its adoption. In that respect, the results are acceptable and satisfying.

Question 2 examined the experts' satisfaction with regard to the number of checklist items included in the USec HE. Results show two *Agree* and one *Disagree* that they are satisfied in this regard. The one *Disagree* score is concerning because it is the opinion of an HCI expert who is knowledgeable about UIMs. Consequently, the number of checklist items included in the HE is an area that will need to be reviewed.

Question 3 examined the length of the USec HE. This question directly relates to Question 2. The results show one *Strongly Agree*, one *Agree* and one *Undecided* with regard to shortening the length of the HE. These results do not exactly align with those in Question 2, except for the opinion of the HCI expert. Therefore these results confirm that the opinion of the HCI expert is correct. As mentioned previously, the length of the HE and the number of checklist items within it is an area that requires more attention in the next iteration phase.

Question 4 examines the ease of use of the USec HE. The results show that two experts *Strongly Agree* and one is *Undecided* about the fact that it is easy to understand and use. The *Undecided* expert is from InfoSec field. Considering this and the background of the other two experts, the ease of use can be regarded acceptable.

Question 5 examines the descriptions of the heuristics. Each heuristic consists of a name and an associated description. Categorised under the heuristic name are the relevant checklist items that operationalise it, which assists experts in understand its application in context. Generally, experts felt that the heuristic descriptions adequately describe what their associated checklist items evaluate. Results show one *Strongly Agree* and two *Agree* on this level. Therefore this aspect is satisfactory.

Question 6 relates to the terminology used in the USec HE. Overall, experts were satisfied with the language. Results show one *Strongly Agree* and two *Agree* scores regarding clear and easy to understand terminology. This shows acceptability.

Question 7 examined the instructions that were provided for the USec HE. The results show that one of the experts *Agree* and two *Disagree* regarding additional instructions to conduct an evaluation. The expert who required additional instructions originates from the InfoSec field. While the instructions provided in the USec HE emulate those of well-known heuristic sets, they include options for the reviewers' answers, comments and severity ratings. The way in which the severity ratings can be applied during the evaluation process was also mentioned. The HCI expert was satisfied with the level of instructions supplied and it can be assumed that this relates to the experts prior experience with this UIM. Based on this, the consensus is that the instructions are sufficient.

Question 8 examined the ease of learning to use the USec HE, as this will impact on the reuse of the tool, which is important because it indirectly demonstrates a successful design. Results show that two experts *Strongly Agree* and one is *Undecided* about the tool's use being easy to remember. The expert that was *Undecided* originates from the InfoSec field and therefore the same rationale applies as to the previous question. It should be noted that an *Undecided* response does not necessarily warrant concern, unless, as in this case, it is expressed by the HCI expert. It can, however, suggest an area that requires more investigation under certain circumstances, as pointed out. Consequently, the tool can be regarded as easy in terms of remembering how it is used.

Question 9 examines the categorisation of checklist items under their heuristics. This question directly relates to Question 5 and the results show that two experts answered *Strongly Agree* and one *Undecided* in this regard and they tend to correlate with those of Question 5. The exception to this is the HCI expert, who was *Undecided* in regard to this question. This means that the categorisation should be reviewed to identify checklist items that fit better under a different heuristic name.

Question 10 examines the usefulness of the amount of information provided in the USec HE. This ensures that the participants are satisfied that the information in checklist items is useful to determine security/privacy usability violations on an interface. The results show that one expert answered *Strongly Agree*, one *Agree* and one *Undecided* for this question. The *Undecided* response was again from the HCI expert; however, there may be a relation with the answers from question 7, where the need for additional instructions was examined. The consensus was that the instructions were sufficient. More information than is required might have been provided to better inform the experts from InfoSec and USec about the HE and how it is used during evaluations. The *Undecided* response from the HCI expert to the current question suggests that the information provided is common knowledge to an HCI expert and some of it could have been excluded. However, as is stated, this question also examines the information in the checklist items. Therefore, the amount of information that is provided in each checklist item should be reviewed in an attempt to eliminate unnecessary information.

As was suggested in previous results, this will also impact on another area that may require improvement – reducing the length of the HE.

Question 11 examines the complexity involved in using the USec HE. This question directly relates to Question 4 and a correlation is found with the results of both questions. The results show that one expert answered *Agree* and two *Disagree* that the USec HE is a complex tool to use. The *Disagree* expert is from InfoSec field; hence, considering this and the background of the other two experts, it can be concluded that it is not a complex tool to use.

Question 12 evaluated the effectiveness of the proposed severity ratings to measure security and privacy usability violations. The results show that two experts *Agree* and one is *Undecided* that the severity ratings are effective. The *Undecided* expert was from the InfoSec field. It is important that the severity ratings are effective because it is their extent that determines where additional usability efforts are a priority in the design. The results of the effectiveness of the severity ratings can therefore be regarded acceptable. However, further investigation should be conducted to guarantee this.

Question 13 focused on the material that was considered for developing the USec HE and evaluated whether the material is sufficient and acceptable. This is a decisive factor for the USec HE, as ensuring that the security and privacy material adequately represents the InfoSec field and that the usability and USec material adequately represents the HCI field is essential. Subsequently, this helps to determine the requirements of each field and consider them in the development of the heuristics and their checklist items. Results show that two experts *Strongly Agree* and one *Agree* that the material is sufficient and acceptable.

Question 14 was not directly focused on the USec HE; instead, it required the experts' opinions concerning the development of USec tools. One of the experts did not provide an answer to this question, while the other two experts stated that it is *Important* to develop such tools.

Question 15 examined the overall quality of the USec HE. The tool can be regarded as one of good quality, as two experts rated it as *Very Good* and one rated it as *Good*. However, making the improvements suggested by the experts in previous questions may be the difference between having a tool that is of very good quality.

Question 16 examined the overall effectiveness of the USec HE. This was deemed to be acceptable, as all three experts rated it *Good*. Once again, the results suggest that the tool can be further improved as mentioned in the previous question.

Question 17 examined the overall usefulness of the USec HE. Accordingly, two experts rated it as *Very Useful* and one as *Useful*. This confirms that it is an effective tool and makes a worthy contribution.

Question 18, which is not included in table 7.16, was an optional question. Experts could provide suggestions for improving the USec HE. One expert mentioned that it is a very good tool but suggested reducing its length. Streamlining it may also reduce its complexity. This was confirmed by the results of Question 3.

The findings obtained from the user satisfaction questionnaire would seem to indicate that the overall results are encouraging, as the effectiveness, quality and usefulness of the tool are more than satisfactory. This suggests that the tool is successful in achieving its intended objectives. Nonetheless, there are areas that can be improved. One concerning factor, however, is the length of the tool and both the experts and the users indicated that the length should be reduced. Other areas for possible improvements that have been suggested but with less emphasis, include

- reviewing the categorisation of checklist items under heuristic names
- removing unnecessary information from the checklist items, which also impacts on length
- reviewing the severity ratings by applying them in context.

7.3 SUMMARY

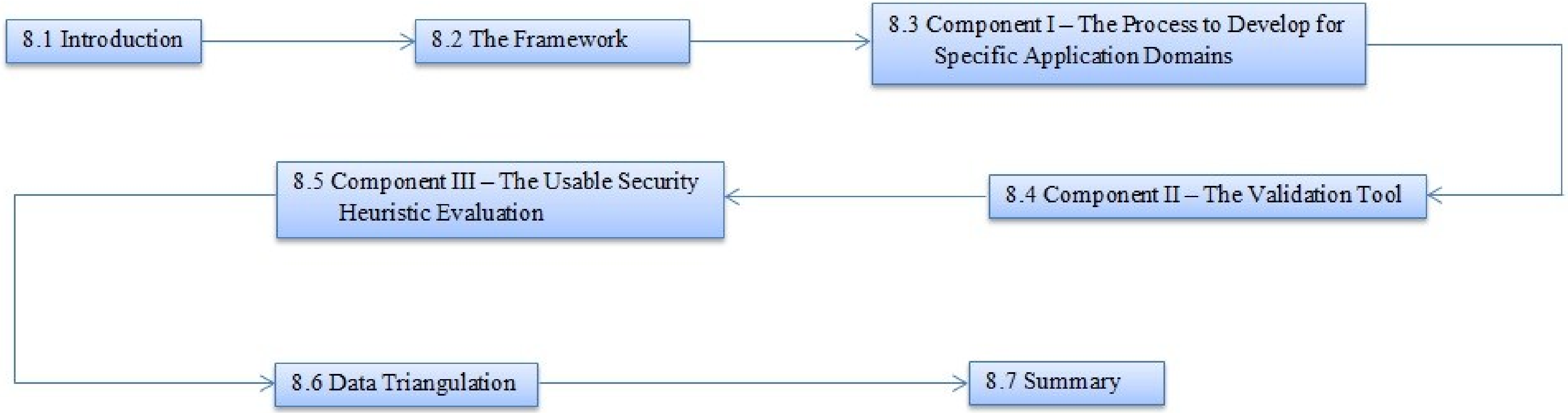
This chapter focuses on the assessments that the experts conducted on the USec HE, for which a validation tool was provided. The validation tool consists of seven sections and comprises a template for evaluating new HEs. All sections of the tool have been discussed in detail in section 7.2 of the chapter. The first section provides instructions for the use and purpose of the tool and the second section is used to collect the biographical data of the experts. The most important information on the experts used in this validation was presented. In the third section of the validation tool, the heuristics were assessed. The main deductions were that the convey features/expressiveness heuristic should be eliminated, while rewording was necessary for the descriptions of five other heuristics.

The fourth section assesses the checklist item of each heuristic, which are categorised within the heuristics that were assessed in section three. An extensive discussion was conducted on the checklist items that did not provide positive ratings or that had specific comments from the experts. The main deductions were that the satisfaction heuristic and seventeen checklist items should be eliminated. Additionally, three new checklist items should be added, eight checklist items should be rephrased, one checklist item should be modified by separating it and two checklist items should be re-grouped. Lastly, three checklist items would be combined into one which would then be re-grouped.

The customised severity ratings are assessed in section five. Between the two severity rating sets presented, the preferred one for measuring USec violations was Set 1. Section six of the validation tool assesses the material that was considered to develop the heuristics and their checklist items. The results indicated that both the usability and USec material and the security and privacy material were not out dated and were particularly relevant.

The seventh and final section of the validation tool comprises a satisfaction questionnaire. Experts provide overall ratings for the new HE, which in this case is intended for USec. The results indicate that the experts had comparable views as those of the participants regarding the USec HE, as it was considered effective in achieving its objectives. Possible improvements would be reducing its length and reviewing the categorisation of checklist items under heuristic names. These were also highlighted in the assessment of checklist items, which is the fourth section of the validation tool. In chapter 8, the framework for USec will be presented.

LAYOUT OF CHAPTER 8


8.1 Introduction
8.2 The Framework
8.3 Component I – The Process to Develop for Specific Application Domains
8.4 Component II – The Validation Tool
8.5 Component III – The Usable Security Heuristic Evaluation
8.6 Data Triangulation
8.7 Summary

CHAPTER 8: APPLICABILITY OF THE USABLE SECURITY FRAMEWORK

8.1 INTRODUCTION

This chapter presents the framework for evaluating USec in online social networking environments. It serves as a proof of concept, illustrating the applicability and use of the proposed framework. It will also mention the supporting instruments of the framework, which include context, components, relationships and outputs.

Section 8.2 will define the framework for the study. In sections 8.3, 8.4 and 8.5, the first, second and third components from the framework will be discussed, respectively. Following, in section 8.6, the research procedures and techniques that were used as part of the data triangulation process are mentioned. The summary is presented in section 8.7.

8.2 THE FRAMEWORK

To determine the applicability of the framework, a series of steps had to be worked through. These were the most significant in the study and they are presented in table 8.1.

Table 8.1: The instrumental steps to construct the framework

#	Step	Resource Required	Result
1	Determine what a conceptual framework is	Literature for frameworks (more focus on conceptual frameworks)	A framework to qualitatively evaluate USec in online social networking
2	Determine the most appropriate UIM for evaluating UI	Literature for HCI (more focus on UIMs)	HE
3	Determine how to develop heuristics	Literature for HCI (more focus on developing heuristics)	Process to develop heuristics for a SAD
4	Develop an HE for evaluating USec on websites/applications	Literature for USec, InfoSec and HCI fields (for HCI more focus on usability and UX, for InfoSec security and privacy)	USec HE
5	Investigate the context in which the USec HE will be applied	Literature for online social networking environments (more focus on OHSNs)	OHSN criteria
6	Determine the OHSNs that will be used for the case study	Apply OHSN criteria	Google Health and MedHelp
7	Determine how to assess the USec HE	Investigate evaluation criteria and Likert scales for designing attitude instruments	Validation tool

Frameworks were discussed in section 5.5 where it was indicated that they concentrate on specific outputs that are produced via the research. To deliver these outputs, a set of research activities must be accomplished, which are instrumental in the research process. For this study, the research activities are defined as the steps presented in table 8.1. Each of the steps had a pivotal role to play in constructing the framework.

From the conceptual framework definition that was provided in section 5.5, the most revealing fact is that it outlines a set of beliefs and theories that support a particular research. This may be a written product that explains in graphical and narrative forms the main aspects of research and elucidates notions such as concepts, variables, factors and relationships, among others (Miles & Huberman, 1994). The thesis provides the evidence representing the theories and beliefs of this particular research and explains it in both narrative and graphical forms. Lethbridge and Laganiere (2005) state that a framework is composed of components and relationships; a view that has been adopted in this study. These authors' diagram of the composition of a framework, which was presented in figure 5.8, has been considered and modified to represent the composition of the framework in this study. The components of a framework to evaluate USec in online social networking environments are presented in figure 8.1.

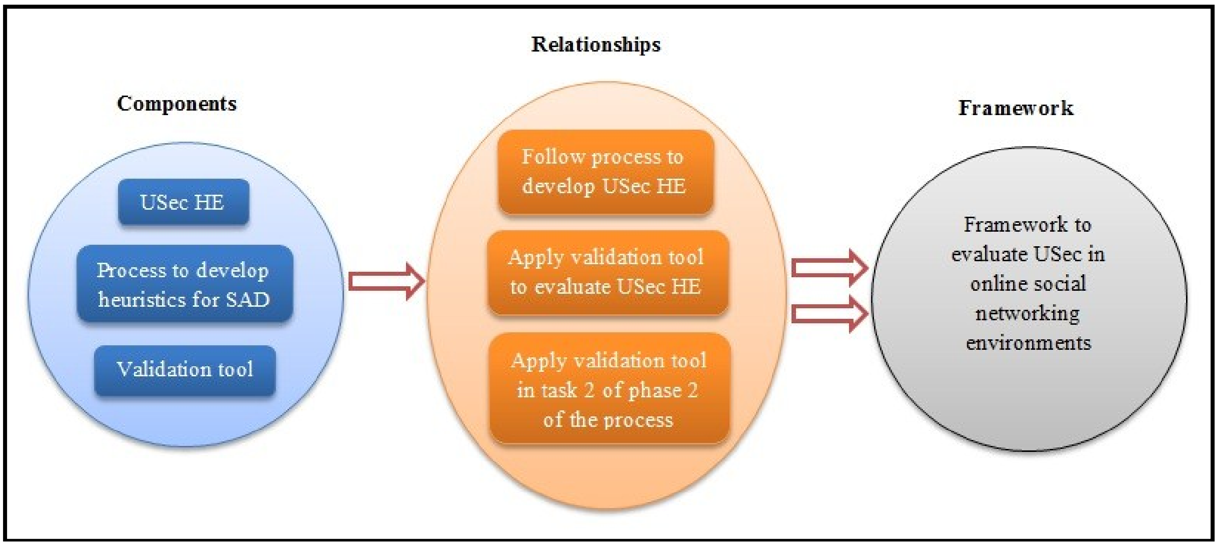

Relationships
Components
Framework
USec HE
Process to develop heuristics for SAD
Validation tool
Follow process to develop USec HE
Apply validation tool to evaluate USec HE
Apply validation tool in task 2 of phase 2 of the process
Framework to evaluate USec in online social networking environments

Figure 8.1: The composition of the framework to evaluate USec in online social networking

The components of the framework, which are illustrated in figure 8.1, are the USec HE, the process to develop heuristics for a SAD and the validation tool. As stated previously, relationships form an integral part of a conceptual framework. Accordingly, there are three fundamental relationships that tie the three components together in this framework:

1. A relationship between the process to develop heuristics for a SAD and the USec HE. To develop the USec HE the process needs to be considered and applied.

2. A relationship between the validation tool and the USec HE. To ensure the applicability and validity of the USec HE, the validation tool had to be applied in order to assess it.
3. A relationship between the process to develop heuristics for a SAD and the validation tool. The validation tool is applied in task 2 of phase 2 in the process of developing heuristics for SADs. Phase 2 and its relevant tasks were discussed in section 4.3.2.

The components and relationships have been established. However, a context is required in which to implement them. This context is online social networking environments. This offers a suitable context, as many non-expert users utilise such environments on a daily basis to connect with other users and share information. However, users are becoming more aware of the implications for not protecting oneself online, USec can nevertheless be an influential contributor in this regard. There are various categories of online social networking websites. These include personal contact management websites (e.g. Facebook), business networking websites (e.g. LinkdIn), cultural trends networking websites (e.g. Twitter) and health websites (Huggins, 2007). In terms of the online social networking context, the category selected for this research is OHSNs.

The components of the framework and their relationships produce specific outputs. In terms of the framework for evaluating USec in online social networking, the components are

1. a process to develop heuristics for SAD
2. a validation tool
3. USec HE

The specific outputs that result from the components relationships are

1. high-level heuristics and checklist items for USec
2. expert feedback to improve Output 1
3. requirements for OHSN
4. USec recommendations for MedHelp and Google Health
5. user feedback to improve Output 1

The context, components and outputs of the USec framework are presented in figure 8.2. In figure 8.2, “O1” stands for “Output 1”; figure 8.3 also illustrates the relationships that are formed within the framework.

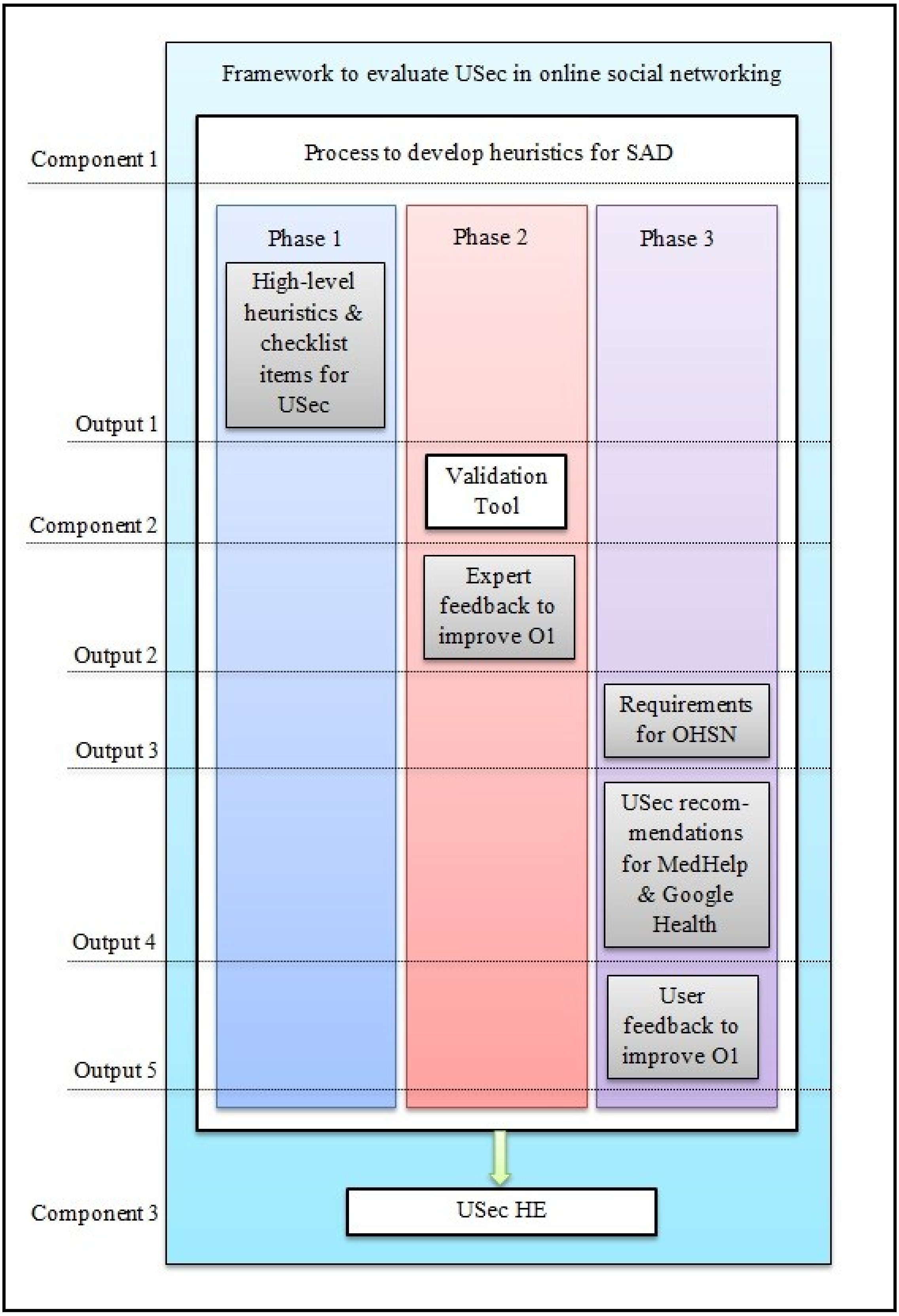

Framework to evaluate USec in online social networking
Component 1
Process to develop heuristics for SAD
Phase 1
Phase 2
Phase 3
High-level heuristics & checklist items for USec
Output 1
Validation Tool
Component 2
Expert feedback to improve O1
Output 2
Requirements for OHSN
Output 3
USec recom-mendations for MedHelp & Google Health
Output 4
User feedback to improve O1
Output 5
Component 3
USec HE

Figure 8.2: The composition of the framework to evaluate USec in online social networking environments in terms of context, components and outputs

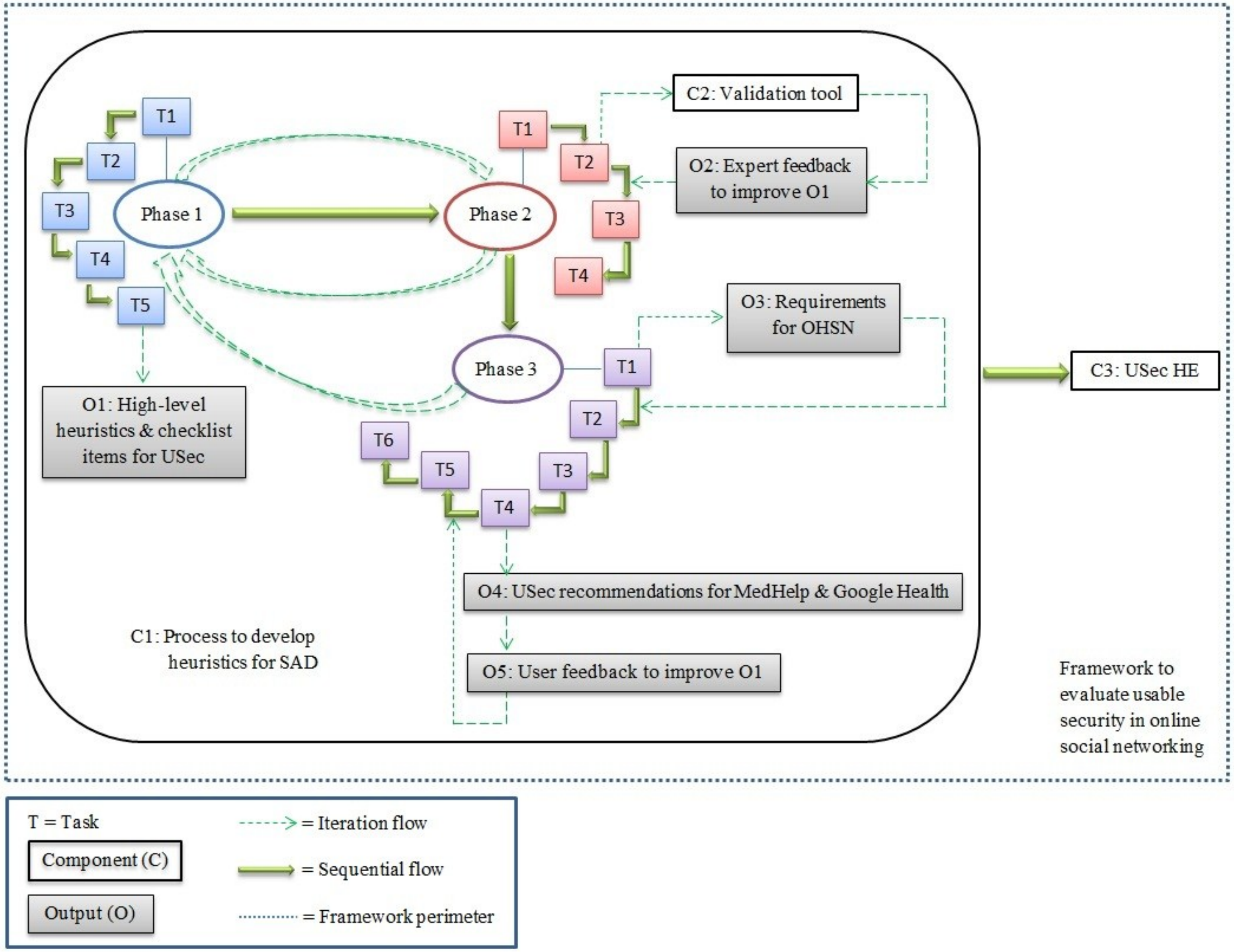

T1
T2
T3
T4
T5
Phase 1
O1: High-level heuristics & checklist items for USec
Phase 2
T1
T2
T3
T4
C2: Validation tool
O2: Expert feedback to improve O1
Phase 3
T1
T2
T3
T4
T5
T6
O3: Requirements for OHSN
O4: USec recommendations for MedHelp & Google Health
O5: User feedback to improve O1
C1: Process to develop heuristics for SAD
C3: USec HE
Framework to evaluate usable security in online social networking
T = Task
Component (C)
Output (O)
= Iteration flow
= Sequential flow
= Framework perimeter

Figure 8.3: The composition of the framework to evaluate USec in online social networking environments in terms of context, components, outputs and relationships

8.3 COMPONENT I – THE PROCESS TO DEVELOP HEURISTICS FOR SAD

The process to develop heuristics for SADs has been discussed in chapter 4. In this section, the three phases of the process will be briefly presented. The purpose is to demonstrate the applicability of the process. This is achieved by explaining what was done in each of the tasks for each phase in order to develop the USec HE. Figure 8.4 presents the tasks for phase 1: Design high-level heuristics.

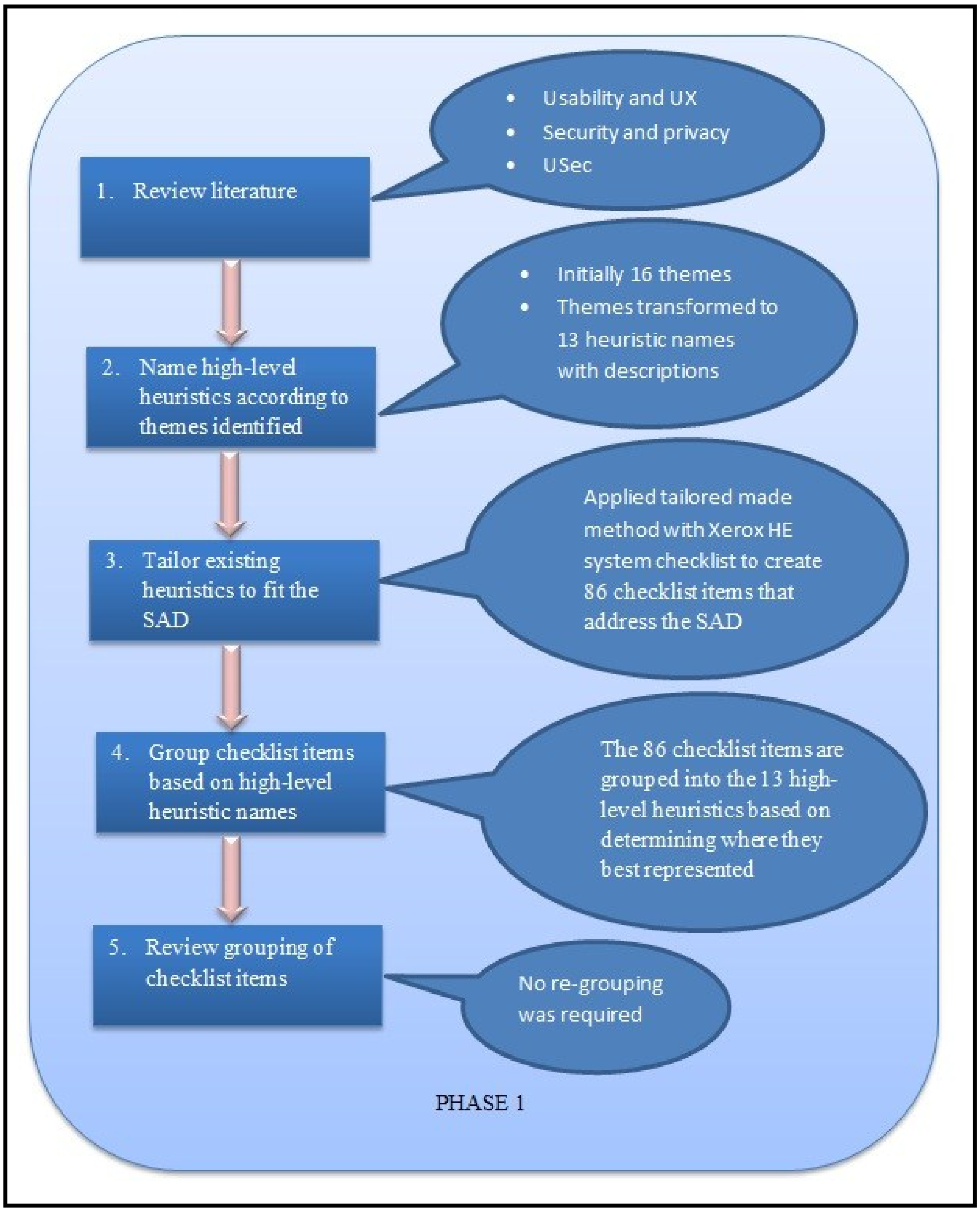

1. Review literature
• Usability and UX
• Security and privacy
• USec
2. Name high-level heuristics according to themes identified
• Initially 16 themes
• Themes transformed to 13 heuristic names with descriptions
3. Tailor existing heuristics to fit the SAD
Applied tailored made method with Xerox HE system checklist to create 86 checklist items that address the SAD
4. Group checklist items based on high-level heuristic names
The 86 checklist items are grouped into the 13 high-level heuristics based on determining where they best represented
5. Review grouping of checklist items
No re-grouping was required
PHASE 1

Figure 8.4: The tasks of phase 1 to develop the USec HE

Phase 1 consists of five tasks:

Task 1 – Review literature: Literature on usability, UX, security, privacy and USec was reviewed.

Task 2 – Name high-level heuristics according to themes identified: From the literature 16 themes were identified. After integrating confidentiality, integrity, availability and privacy into a single theme (security and privacy), 13 high-level heuristics with descriptions resulted.
Task 3 – Tailor existing heuristics to fit the SAD: The Xerox HE system checklist was applied for the tailored made method. This resulted in 86 checklist items that could address the SAD.
Task 4 – Group checklist items based on high-level heuristic names: The 86 checklist items were categorised under the 13 high-level heuristics.
Task 5 – Review grouping of checklist items: Following the grouping of the checklist items into their respective high-level heuristics, a review was conducted. The outcome was that no re-grouping was required.

Phase 2: Validation of high-level heuristics consists of four tasks, which are presented in figure 8.5:
Task 1 – Identify and select experts: The experts selected included two from InfoSec, one from HCI and one from USec.
Task 2 – Apply validation tool to validate high-level heuristics: Experts applied the validation tool to assess the USec HE. The tool included seven sheets in total. Sheet one comprised the instructions, which are not illustrated in figure 8.4. The validation tool will be discussed in more detail in section 8.4 since it is a component of the framework.
Task 3 – Analyse review results: The results from the validation tool were interpreted, analysed and conclusions were made. These were discussed in chapter 7.
Task 4 – Iterate and re-design high-level heuristics: Based on the conclusions made in the previous task, areas for improvements were defined, as presented in figure 8.4. The rephrasing of eight checklist item required the process to iterate to tasks 1 (Literature review) and 3 (Tailor existing heuristics to fit the SAD) of phase 1. The modification of one checklist item required the process of iterating to task 1 (Literature review) of phase 1. The re-grouping of three checklist items required the process to iterate to tasks 4 (Group checklist items based on high-level heuristic names) and 5 (Review grouping of checklist items) of phase 1 respectively.

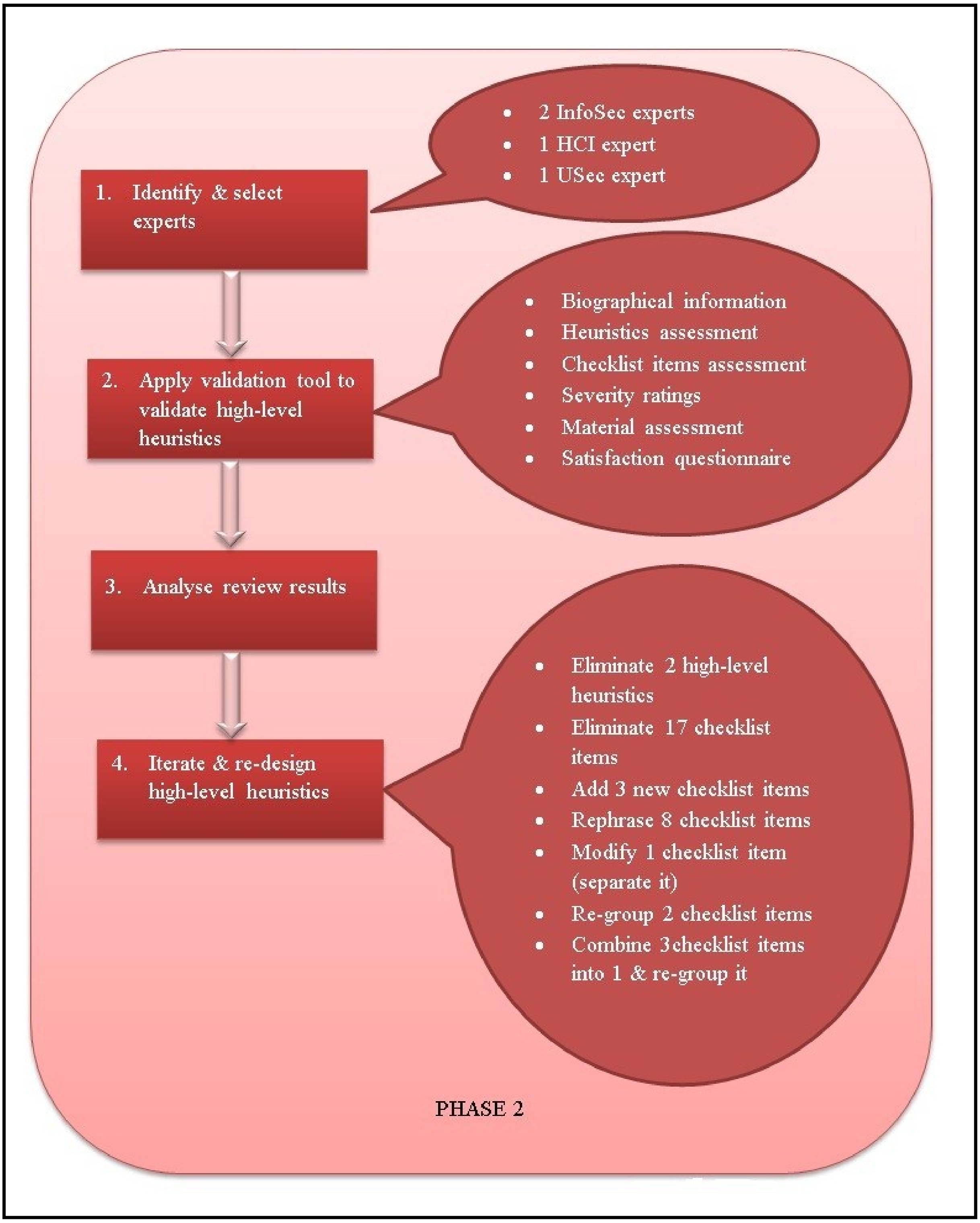

1. Identify & select experts
2 InfoSec experts
1 HCI expert
1 USec expert
2. Apply validation tool to validate high-level heuristics
Biographical information
Heuristics assessment
Checklist items assessment
Severity ratings
Material assessment
Satisfaction questionnaire
3. Analyse review results
4. Iterate & re-design high-level heuristics
Eliminate 2 high-level heuristics
Eliminate 17 checklist items
Add 3 new checklist items
Rephrase 8 checklist items
Modify 1 checklist item (separate it)
Re-group 2 checklist items
Combine 3checklist items into 1 & re-group it
PHASE 2

Figure 8.5: The tasks of phase 2 to develop the USec HE

Figure 8.6 presents the tasks for phase 3: Application of high-level heuristics.

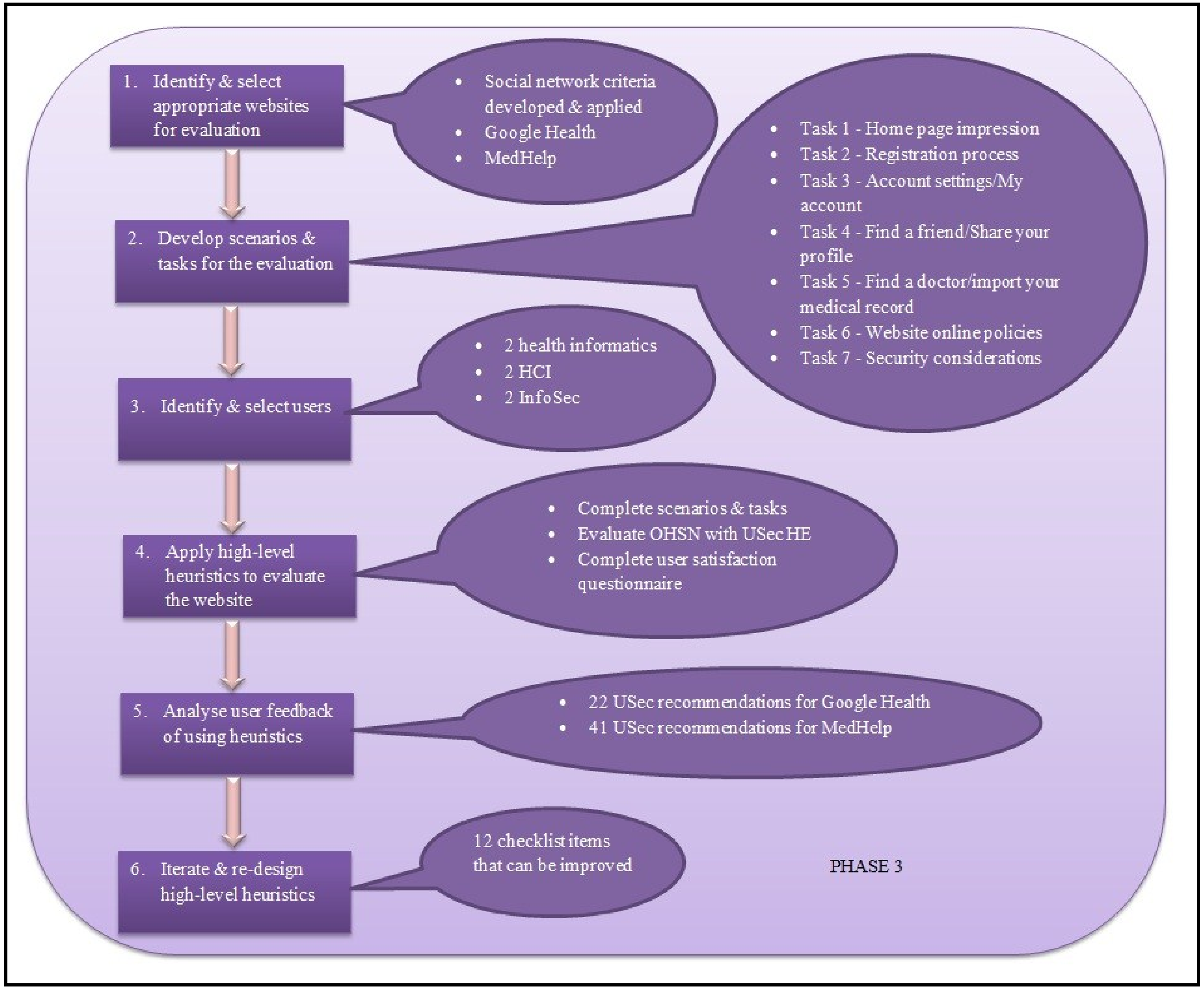

1. Identify & select appropriate websites for evaluation
• Social network criteria developed & applied
• Google Health
• MedHelp
2. Develop scenarios & tasks for the evaluation
• Task 1 - Home page impression
• Task 2 - Registration process
• Task 3 - Account settings/My account
• Task 4 - Find a friend/Share your profile
• Task 5 - Find a doctor/import your medical record
• Task 6 - Website online policies
• Task 7 - Security considerations
3. Identify & select users
• 2 health informatics
• 2 HCI
• 2 InfoSec
4. Apply high-level heuristics to evaluate the website
• Complete scenarios & tasks
• Evaluate OHSN with USec HE
• Complete user satisfaction questionnaire
5. Analyse user feedback of using heuristics
• 22 USec recommendations for Google Health
• 41 USec recommendations for MedHelp
6. Iterate & re-design high-level heuristics
12 checklist items that can be improved
PHASE 3

Figure 8.6: The tasks of phase 3 to develop the USec HE

Phase 3 consists of six tasks:

Task 1 – Identify and select appropriate websites for evaluation: Social network criteria were established to assess a number of OHSNs. Based on the procedure, Google Health and MedHelp were selected.

Task 2 – Develop scenarios and tasks for the evaluation: Participants were provided with scenarios, which required them to complete seven main tasks. The tasks are illustrated in figure 8.5.

Task 3 – Identify and select users: Six participants were selected. These were postgraduate students; two from health informatics, two from HCI and two from InfoSec.

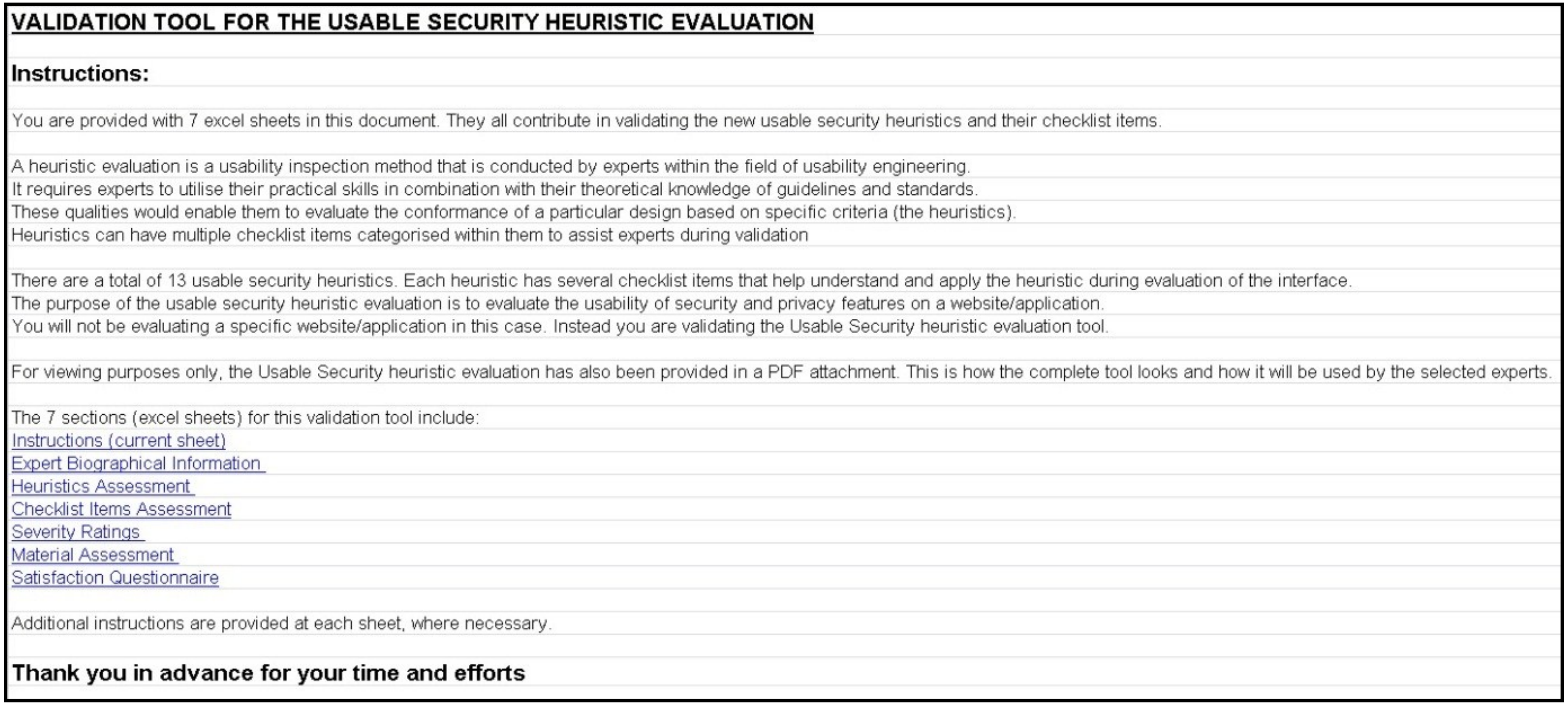
Task 4 – Apply high-level heuristics to evaluate the website: Upon completing the scenarios and tasks, the participants applied the USec HE to evaluate the OHSN. Once this was done, they completed a user satisfaction questionnaire.

Task 5 – Analyse user feedback of using heuristics: The results from the evaluation were analysed and the outcome was 22 USec recommendations for Google Health and 41 for MedHelp. These were mentioned in chapter 6.

Task 6 – Iterate and re-design high-level heuristics: From the perspective of the USec HE, twelve improvements were suggested by the participants. Most related to the re-phrasing of the checklist items, which required the process to iterate to tasks 1 (Literature review) and 3 (Tailor existing heuristics to fit the SAD) of phase 1. In addition, the checklist items suggested for improvement were compared against the experts' assessments of them.

8.4 COMPONENT II – THE VALIDATION TOOL

The analysis of the validation tool results were discussed in chapter 7. The validation tool is applied in task 2 of phase 2 of the process. As mentioned previously, there are seven sheets included in the tool and each of these will be presented in this section. The validation tool is customised for USec; however, it can be used as a template for creating similar validation tools. The tool would be modified to evaluate the heuristics of a SAD for which they are being developed (see *Appendix A.2: Validation Tool Template*). The descriptions of each sheet will follow. Sheet 1 provides the instructions. These should explain the purpose of the tool and of the overall research. The sheet includes basic instructions on how the tool will be used, since there are specific instructions on each sheet. Additionally, the sheet has links to all other sheets in the tool. It is advisable to send the HE created as a separate document, as it provides experts with a view of the proposed complete tool. Sheet 1 is presented in figure 8.7.



VALIDATION TOOL FOR THE USABLE SECURITY HEURISTIC EVALUATION

Instructions:

You are provided with 7 excel sheets in this document. They all contribute in validating the new usable security heuristics and their checklist items.

A heuristic evaluation is a usability inspection method that is conducted by experts within the field of usability engineering.
It requires experts to utilise their practical skills in combination with their theoretical knowledge of guidelines and standards.
These qualities would enable them to evaluate the conformance of a particular design based on specific criteria (the heuristics).
Heuristics can have multiple checklist items categorised within them to assist experts during validation

There are a total of 13 usable security heuristics. Each heuristic has several checklist items that help understand and apply the heuristic during evaluation of the interface.
The purpose of the usable security heuristic evaluation is to evaluate the usability of security and privacy features on a website/application.
You will not be evaluating a specific website/application in this case. Instead you are validating the Usable Security heuristic evaluation tool.

For viewing purposes only, the Usable Security heuristic evaluation has also been provided in a PDF attachment. This is how the complete tool looks and how it will be used by the selected experts.

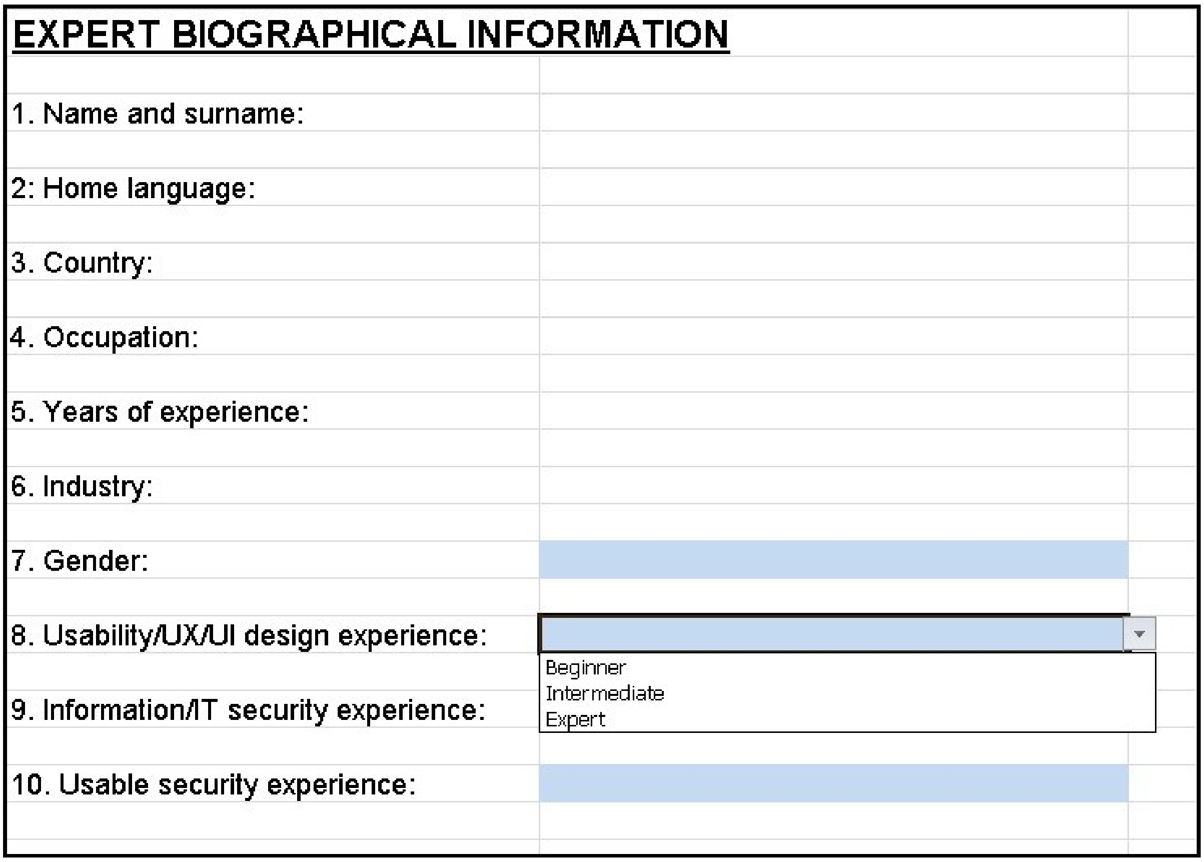
The 7 sections (excel sheets) for this validation tool include:
Instructions (current sheet)
Expert Biographical Information
Heuristics Assessment
Checklist Items Assessment
Severity Ratings
Material Assessment
Satisfaction Questionnaire

Additional instructions are provided at each sheet, where necessary.

Thank you in advance for your time and efforts

Figure 8.7: Sheet 1 of the validation tool (see sheet 1 of *Appendix A.2: Validation Tool Template*)

Sheet 2 is used to collect the experts' biographical information and includes the basic information required for this study. More information can be included and collected, depending on the study. The first seven items are quite general, while items eight, nine and ten are for the SAD. These items would most likely be modified when creating heuristics for another SAD, unless the HCI, InfoSec or USec form part of the SAD. In that case, that item would remain in the sheet. Sheet 2 is presented in figure 8.8.



EXPERT BIOGRAPHICAL INFORMATION

1. Name and surname:

2: Home language:

3. Country:

4. Occupation:

5. Years of experience:

6. Industry:

7. Gender:

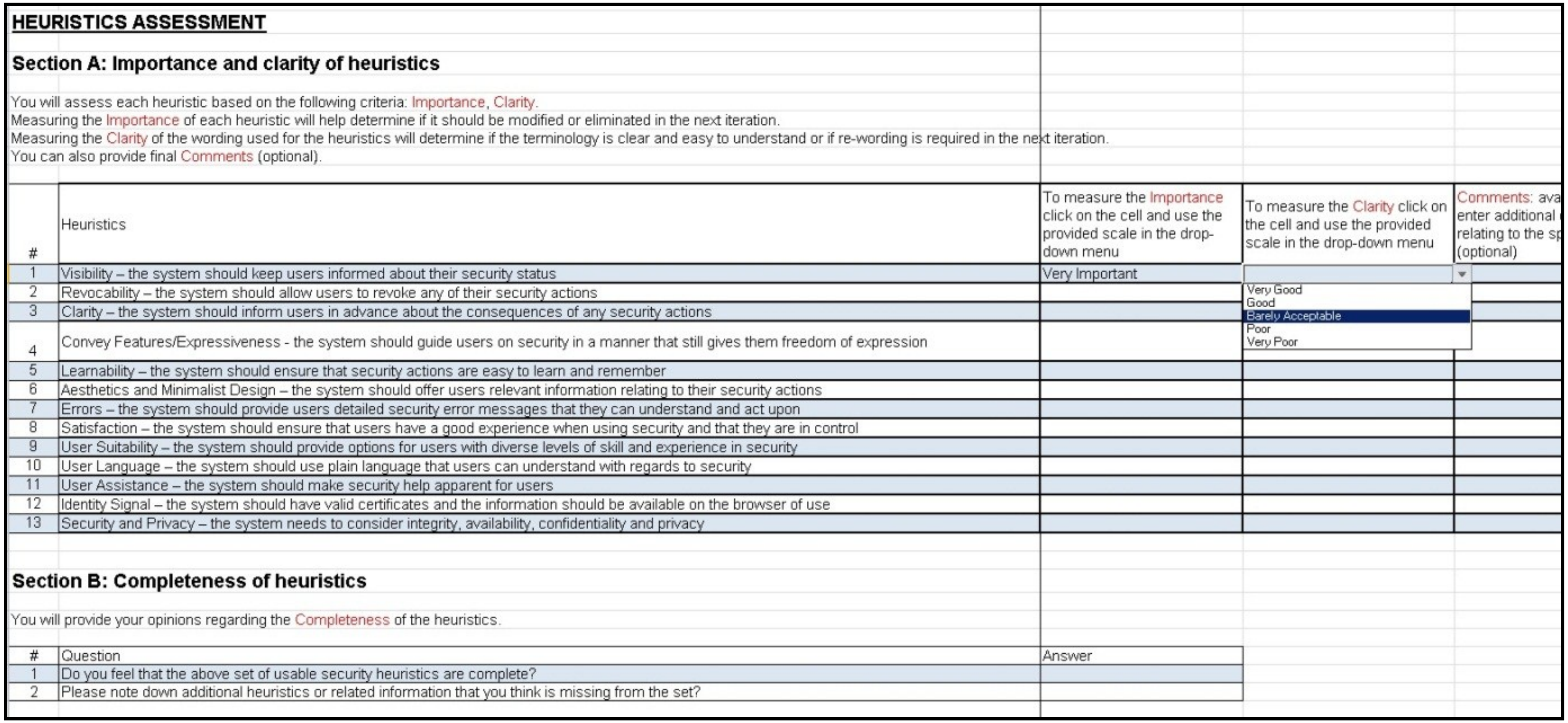
8. Usability/UX/UI design experience:

9. Information/IT security experience:

10. Usable security experience:

Figure 8.8: Sheet 2 of the validation tool (see sheet 2 of *Appendix A.2: Validation Tool Template*)

Sheet 3 is used to assess the high-level heuristics and their descriptions. In section A importance and clarity are measured. In addition, experts may provide optional comments at each heuristic. Section B is used to determine the completeness of the heuristic set. A part of Sheet 3 is presented in figure 8.9. Sheet 4 measures the checklist items for each of the high-level heuristics from sheet 3. These are measured for clarity, grouping and relevance. Experts then provide a final verdict on the inclusion of the item and can also provide optional comments for each item. The completeness of the checklist items for a high-level heuristic are then determined. A part of Sheet 4 is presented in figure 8.10.



HEURISTICS ASSESSMENT

Section A: Importance and clarity of heuristics

You will assess each heuristic based on the following criteria: Importance, Clarity.
Measuring the Importance of each heuristic will help determine if it should be modified or eliminated in the next iteration.
Measuring the Clarity of the wording used for the heuristics will determine if the terminology is clear and easy to understand or if re-wording is required in the next iteration.
You can also provide final Comments (optional).

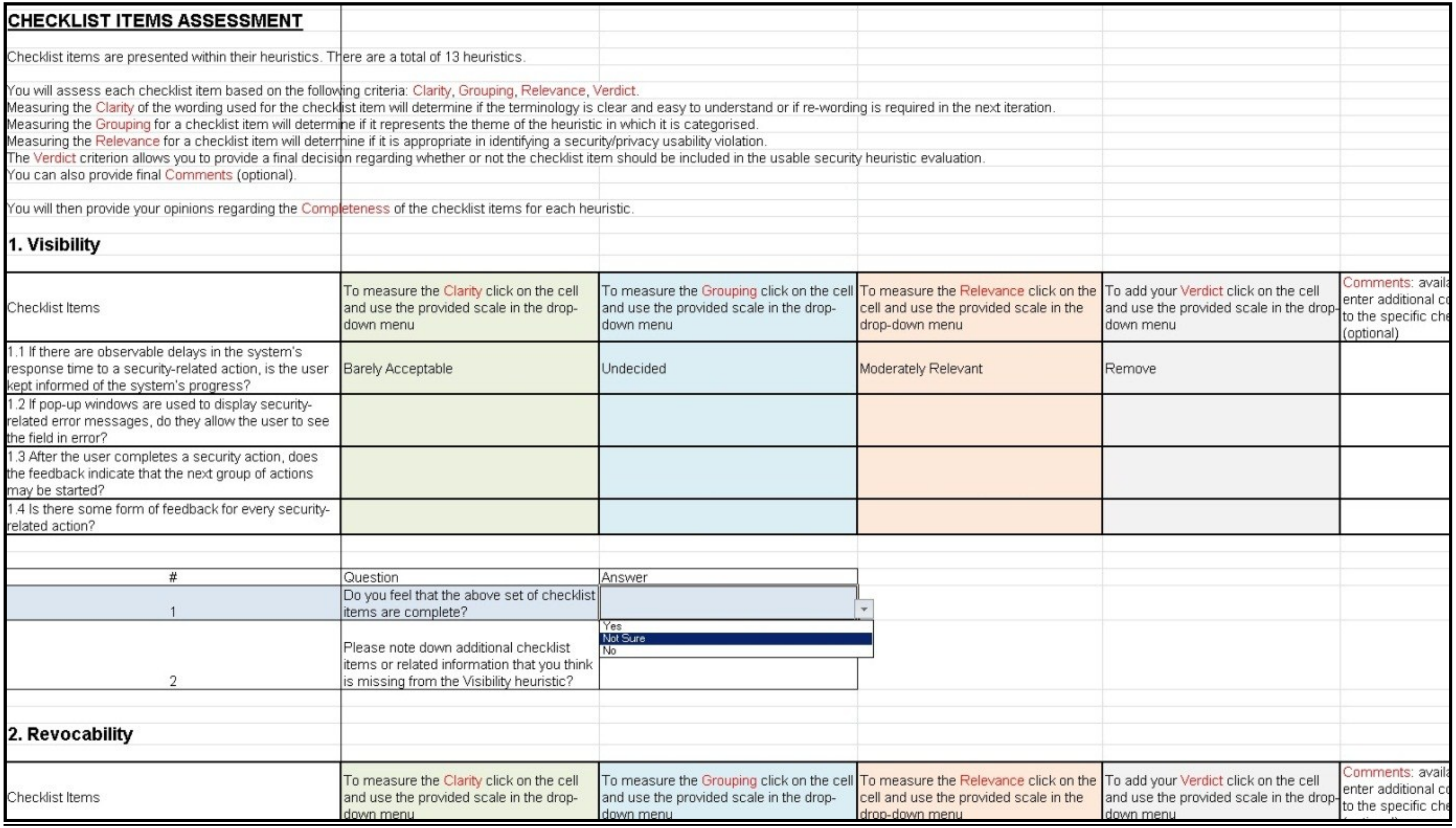
#	Heuristics	To measure the Importance click on the cell and use the provided scale in the drop-down menu	To measure the Clarity click on the cell and use the provided scale in the drop-down menu	Comments: ava enter additional relating to the sp (optional)
1	Visibility – the system should keep users informed about their security status	Very Important		
2	Revocability – the system should allow users to revoke any of their security actions			
3	Clarity – the system should inform users in advance about the consequences of any security actions			
4	Convey Features/Expressiveness - the system should guide users on security in a manner that still gives them freedom of expression			
5	Learnability – the system should ensure that security actions are easy to learn and remember			
6	Aesthetics and Minimalist Design – the system should offer users relevant information relating to their security actions			
7	Errors – the system should provide users detailed security error messages that they can understand and act upon			
8	Satisfaction – the system should ensure that users have a good experience when using security and that they are in control			
9	User Suitability – the system should provide options for users with diverse levels of skill and experience in security			
10	User Language – the system should use plain language that users can understand with regards to security			
11	User Assistance – the system should make security help apparent for users			
12	Identity Signal – the system should have valid certificates and the information should be available on the browser of use			
13	Security and Privacy – the system needs to consider integrity, availability, confidentiality and privacy			

Section B: Completeness of heuristics

You will provide your opinions regarding the Completeness of the heuristics.

#	Question	Answer
1	Do you feel that the above set of usable security heuristics are complete?	
2	Please note down additional heuristics or related information that you think is missing from the set?	

Figure 8.9: Part of Sheet 3 of the validation tool (see sheet 3 of *Appendix A.2: Validation Tool Template*)



CHECKLIST ITEMS ASSESSMENT

Checklist items are presented within their heuristics. There are a total of 13 heuristics.

You will assess each checklist item based on the following criteria: Clarity, Grouping, Relevance, Verdict.
Measuring the Clarity of the wording used for the checklist item will determine if the terminology is clear and easy to understand or if re-wording is required in the next iteration.
Measuring the Grouping for a checklist item will determine if it represents the theme of the heuristic in which it is categorised.
Measuring the Relevance for a checklist item will determine if it is appropriate in identifying a security/privacy usability violation.
The Verdict criterion allows you to provide a final decision regarding whether or not the checklist item should be included in the usable security heuristic evaluation.
You can also provide final Comments (optional).

You will then provide your opinions regarding the Completeness of the checklist items for each heuristic.

1. Visibility

Checklist Items	To measure the Clarity click on the cell and use the provided scale in the drop-down menu	To measure the Grouping click on the cell and use the provided scale in the drop-down menu	To measure the Relevance click on the cell and use the provided scale in the drop-down menu	To add your Verdict click on the cell and use the provided scale in the drop-down menu	Comments: avail enter additional c to the specific che (optional)
1.1 If there are observable delays in the system's response time to a security-related action, is the user kept informed of the system's progress?	Barely Acceptable	Undecided	Moderately Relevant	Remove	
1.2 If pop-up windows are used to display security-related error messages, do they allow the user to see the field in error?					
1.3 After the user completes a security action, does the feedback indicate that the next group of actions may be started?					
1.4 Is there some form of feedback for every security-related action?					

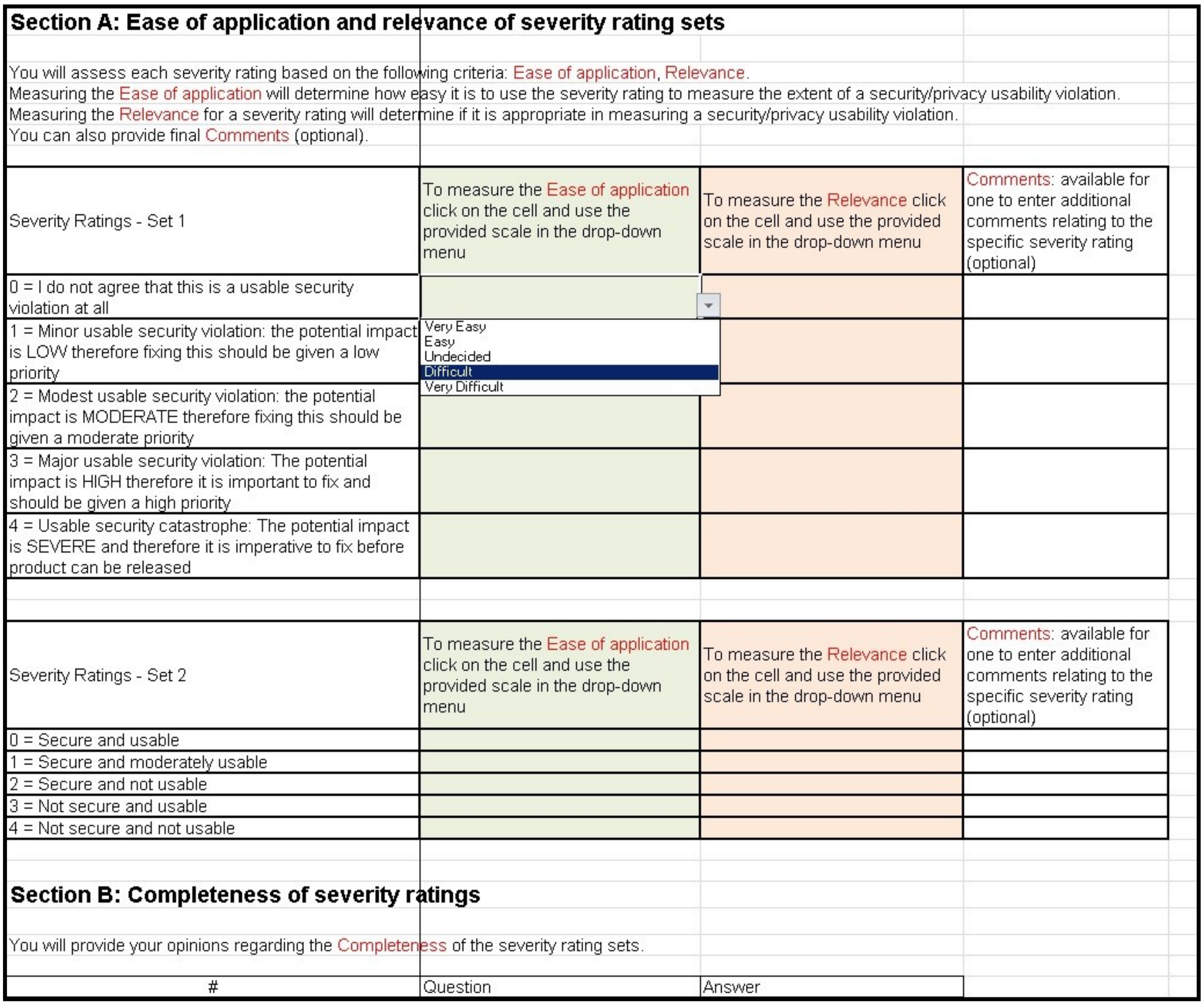
#	Question	Answer
1	Do you feel that the above set of checklist items are complete?	
2	Please note down additional checklist items or related information that you think is missing from the Visibility heuristic?	

2. Revocability

Checklist Items	To measure the Clarity click on the cell and use the provided scale in the drop-down menu	To measure the Grouping click on the cell and use the provided scale in the drop-down menu	To measure the Relevance click on the cell and use the provided scale in the drop-down menu	To add your Verdict click on the cell and use the provided scale in the drop-down menu	Comments: avail enter additional c to the specific che

Figure 8.10: Part of Sheet 4 of the validation tool (see sheet 4 of *Appendix A.2: Validation Tool Template*)

Sheet 5 is used to assess the customised severity ratings for a new HE. This sheet is only included if customised severity ratings are required. Otherwise, the severity ratings of well-known heuristic sets can be applied (e.g. Nielsen's severity ratings) and this sheet will be excluded. In the case of this study, two sets of customised severity ratings were assessed for ease of application and relevance in section A. Experts can also provide optional comments for each rating in the set. Section B is used to determine the completeness of each severity rating set, while in section C, experts provide their preference for a severity rating set to measure USec violations. Part of Sheet 5 is presented in figure 8.11.



Section A: Ease of application and relevance of severity rating sets

You will assess each severity rating based on the following criteria: Ease of application, Relevance.
Measuring the Ease of application will determine how easy it is to use the severity rating to measure the extent of a security/privacy usability violation.
Measuring the Relevance for a severity rating will determine if it is appropriate in measuring a security/privacy usability violation.
You can also provide final Comments (optional).

Severity Ratings - Set 1	To measure the Ease of application click on the cell and use the provided scale in the drop-down menu	To measure the Relevance click on the cell and use the provided scale in the drop-down menu	Comments: available for one to enter additional comments relating to the specific severity rating (optional)
0 = I do not agree that this is a usable security violation at all			
1 = Minor usable security violation: the potential impact is LOW therefore fixing this should be given a low priority			
2 = Modest usable security violation: the potential impact is MODERATE therefore fixing this should be given a moderate priority			
3 = Major usable security violation: The potential impact is HIGH therefore it is important to fix and should be given a high priority			
4 = Usable security catastrophe: The potential impact is SEVERE and therefore it is imperative to fix before product can be released			

Severity Ratings - Set 2	To measure the Ease of application click on the cell and use the provided scale in the drop-down menu	To measure the Relevance click on the cell and use the provided scale in the drop-down menu	Comments: available for one to enter additional comments relating to the specific severity rating (optional)
0 = Secure and usable			
1 = Secure and moderately usable			
2 = Secure and not usable			
3 = Not secure and usable			
4 = Not secure and not usable			

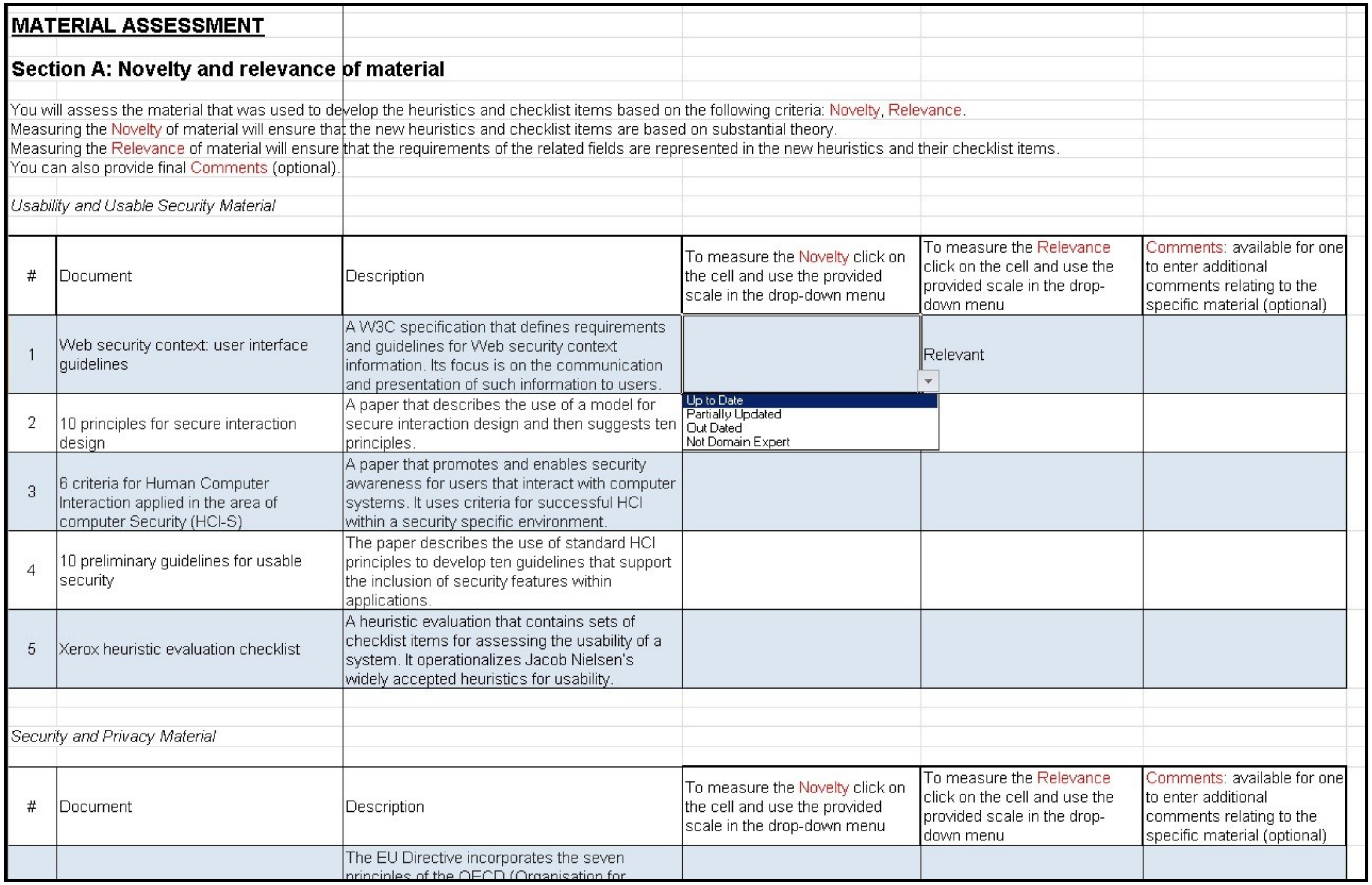
Section B: Completeness of severity ratings

You will provide your opinions regarding the Completeness of the severity rating sets.

#	Question	Answer

Figure 8.11: Part of Sheet 5 of the validation tool (see sheet 5 of *Appendix A.2: Validation Tool Template*)

Sheet 6 is used to assess the material considered to develop high-level heuristics and their checklist items. Materials are assessed for novelty and relevance in section A. Experts can also provide optional comments for each piece of material. Section B is used to determine the completeness of the materials. In this study, two sets of materials were considered: the first set being usability and USec material and the second set security and privacy material. Sheet 6 is presented in figure 8.12.



MATERIAL ASSESSMENT

Section A: Novelty and relevance of material

You will assess the material that was used to develop the heuristics and checklist items based on the following criteria: Novelty, Relevance.
Measuring the Novelty of material will ensure that the new heuristics and checklist items are based on substantial theory.
Measuring the Relevance of material will ensure that the requirements of the related fields are represented in the new heuristics and their checklist items.
You can also provide final Comments (optional).

Usability and Usable Security Material

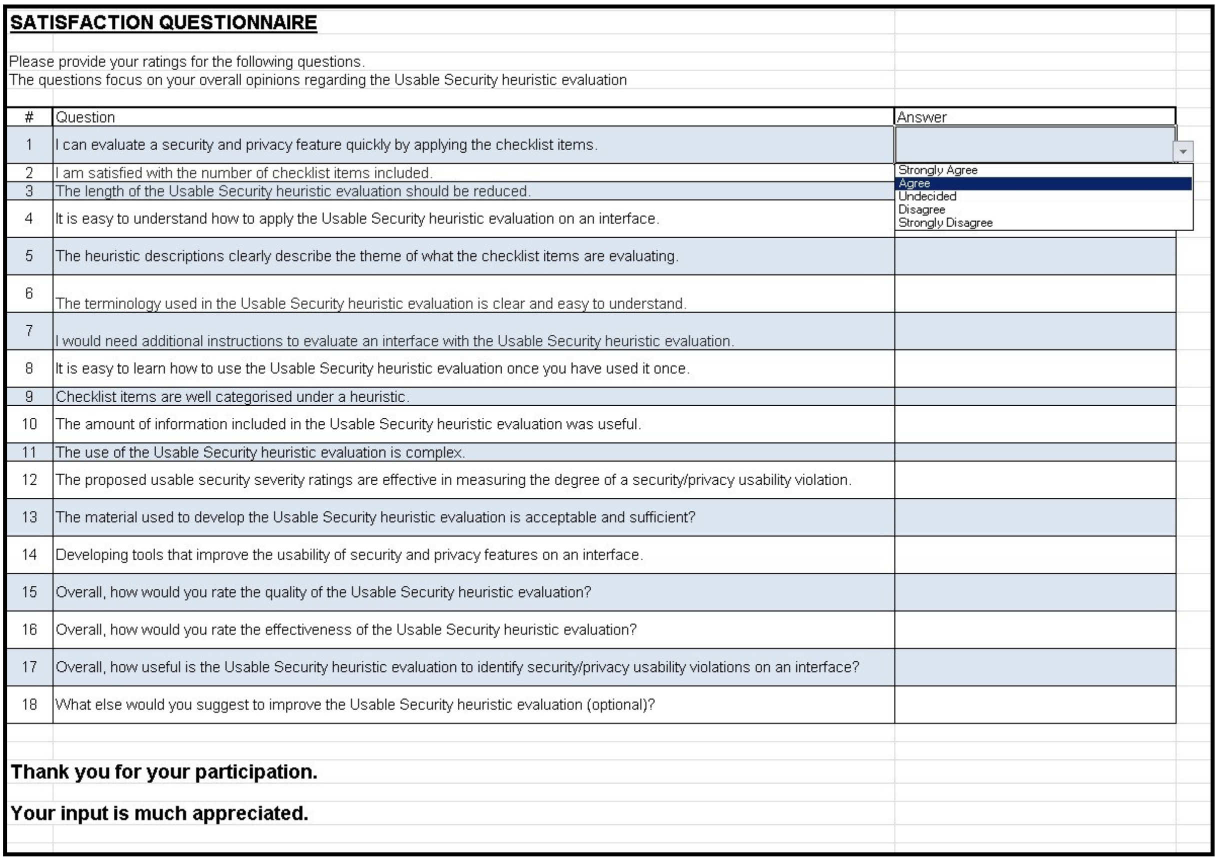
#	Document	Description	To measure the Novelty click on the cell and use the provided scale in the drop-down menu	To measure the Relevance click on the cell and use the provided scale in the drop-down menu	Comments: available for one to enter additional comments relating to the specific material (optional)
1	Web security context: user interface guidelines	A W3C specification that defines requirements and guidelines for Web security context information. Its focus is on the communication and presentation of such information to users.		Relevant	
2	10 principles for secure interaction design	A paper that describes the use of a model for secure interaction design and then suggests ten principles.			
3	6 criteria for Human Computer Interaction applied in the area of computer Security (HCI-S)	A paper that promotes and enables security awareness for users that interact with computer systems. It uses criteria for successful HCI within a security specific environment.			
4	10 preliminary guidelines for usable security	The paper describes the use of standard HCI principles to develop ten guidelines that support the inclusion of security features within applications.			
5	Xerox heuristic evaluation checklist	A heuristic evaluation that contains sets of checklist items for assessing the usability of a system. It operationalizes Jacob Nielsen's widely accepted heuristics for usability.			

Security and Privacy Material

#	Document	Description	To measure the Novelty click on the cell and use the provided scale in the drop-down menu	To measure the Relevance click on the cell and use the provided scale in the drop-down menu	Comments: available for one to enter additional comments relating to the specific material (optional)
		The EU Directive incorporates the seven principles of the OECD (Organisation for			

Figure 8.12: Part of Sheet 6 of the validation tool (see sheet 6 of *Appendix A.2: Validation Tool Template*)

Sheet 7 is a satisfaction questionnaire. The experts will provide their overall opinions on the new HE on this sheet. Sheet 7 is presented in figure 8.13.



SATISFACTION QUESTIONNAIRE

Please provide your ratings for the following questions.
The questions focus on your overall opinions regarding the Usable Security heuristic evaluation

#	Question	Answer
1	I can evaluate a security and privacy feature quickly by applying the checklist items.	
2	I am satisfied with the number of checklist items included.	
3	The length of the Usable Security heuristic evaluation should be reduced.	
4	It is easy to understand how to apply the Usable Security heuristic evaluation on an interface.	
5	The heuristic descriptions clearly describe the theme of what the checklist items are evaluating.	
6	The terminology used in the Usable Security heuristic evaluation is clear and easy to understand.	
7	I would need additional instructions to evaluate an interface with the Usable Security heuristic evaluation.	
8	It is easy to learn how to use the Usable Security heuristic evaluation once you have used it once.	
9	Checklist items are well categorised under a heuristic.	
10	The amount of information included in the Usable Security heuristic evaluation was useful.	
11	The use of the Usable Security heuristic evaluation is complex.	
12	The proposed usable security severity ratings are effective in measuring the degree of a security/privacy usability violation.	
13	The material used to develop the Usable Security heuristic evaluation is acceptable and sufficient?	
14	Developing tools that improve the usability of security and privacy features on an interface.	
15	Overall, how would you rate the quality of the Usable Security heuristic evaluation?	
16	Overall, how would you rate the effectiveness of the Usable Security heuristic evaluation?	
17	Overall, how useful is the Usable Security heuristic evaluation to identify security/privacy usability violations on an interface?	
18	What else would you suggest to improve the Usable Security heuristic evaluation (optional)?	

Thank you for your participation.

Your input is much appreciated.

Figure 8.13: Sheet 7 of the validation tool (see sheet 7 of *Appendix A.2: Validation Tool Template*)

8.5 COMPONENT III – THE USEC HE

The USec heuristics and checklist items from the first iteration were presented in chapter 4. Based on the analysis of the experts' validation tools and the participant comments made during the application of the USec HE, some modifications and improvements have been made. Table 8.2 presents the final heuristics and checklist items for USec, which are the result of the second iteration. This is an improvement from the first iteration, as presented in table 4.3. A template of the complete USec HE with severity ratings is provided in *Appendix A.1: USec HE*. It is important to note that the term *user* in the USec HE defines an intended user of the website/application (e.g. a hacker is not considered as an intended user).

Table 8.2: The USec HE after second iteration (see *Appendix A.1: USec HE*)

1. Visibility – the system should keep users informed about their security status
1.1 If there are observable delays in the system's response time to a security-related action, is the user kept informed of the system's progress?
1.2 Are security-related error messages displayed next to the field in question?
1.3 After the user completes a security action, does the feedback indicate that the next group of actions may be started?
1.4 Is there some form of feedback for every security-related action?
1.5 Is the user's status on the system visible (e.g. who is logged in, what level of privileges, timeout)?
1.6 By looking, can the user tell the security state of the system, and the alternatives for security-related actions, if needed?
2. Revocability – the system should allow users to revoke security actions where appropriate
2.1 Do security options in menus make obvious whether de-selection is possible?
2.2 Can users easily reverse their security actions where possible? If not, does the system provide a compensating action?
2.3 When prompts imply a necessary security action, are the words in the message consistent with that action?
2.4 Has the system been designed so that keys with similar names are not close to each other and do not perform opposite (and potentially dangerous) security actions (e.g. send vs. save information)?
3. Clarity – the system should inform users in advance about the consequences of any security actions
3.1 Are users prompt in confirming security actions that have drastic, destructive consequences?
3.2 Does the system warn users if they are about to make a potentially serious security error (e.g. make their pictures accessible to all users)?
3.3 Does the system prevent users from making security errors whenever possible (e.g. make their entire profile accessible to all users)?
3.4 Does the system clearly explain why a security action must be taken and what are the risks of not taking it?
4. Learnability – the system should ensure that security actions are easy to learn and remember
4.1 Have security items been grouped into logical zones, and have headings been used to distinguish between the zones?
4.2 Does the system provide mapping: that is, are the relationships between security controls and security actions apparent to the user?
4.3 Are security operations easy to learn?
4.4 Are security operations easy to use?
4.5 Are users informed about their security selection defaults (if they exist) during their first interaction?
4.6 Do GUI menus make obvious which security items are selected?
4.7 Does the system protect users from making severe errors?
4.8 Is security-related information presented in a standardised manner within the individual system?
5. Aesthetics and Minimalist Design – the system should apply appropriate visual representation of security elements and not provide irrelevant security information
5.1 Is only security information which is relevant to the user displayed on the screen?
5.2 Are all security icons in a set visually and conceptually distinct?
5.3 Are security labels brief, familiar and descriptive?
5.4 Are security prompts expressed in the affirmative (e.g. would you like to check your default settings?)?

5.5 Are there visual privacy indicators informing users about the privacy practices of the system?
6. Errors – the system should provide users detailed security error messages that they can understand and act upon to recover
6.1 Are security-related prompts stated constructively, without overt criticism of the user?
6.2 Do security-related error messages inform the user of the error's severity?
6.3 Do security-related error messages suggest the cause of the problem?
6.4 Do security-related error messages indicate what action the user needs to take to correct the error?
6.5 Are the security-related error messages accurate in their descriptions?
7. User Suitability – the system should provide options for users with diverse levels of skill and experience in security
7.1. Are multiple levels of security error message detail available?
7.2 Can users choose between iconic and text display of security information, where appropriate?
7.3 Are multiple levels of security detail available?
7.4 Can users customise security to meet their individual preferences?
8. User Language – the system should use plain language that users can understand with regard to security
8.1 Are security actions named consistently across all prompts in the design (e.g. using security action messages to block a user)?
8.2 Are security objects named consistently across all prompts in the design (e.g. using the block icon/tab to block a user)?
8.3 Is security information accurate, complete and understandable?
8.4 Are security questions stated in clear and simple language, where used?
8.5 Is privacy jargon avoided (e.g. information in the privacy policy)?
8.6 Is security jargon avoided (e.g. information for security handling in policies)?
9. User Assistance – the system should make security help relevant and apparent to users
9.1 Is there a security help function visible (e.g. a key labelled "Security Help")?
9.2 Is the security information provided relevant?
9.3 Can users easily switch between security help and their tasks?
9.4 Do instructions follow the sequence of user security actions?
9.5 Does the system provide users with opportunities for updated security education, if they desire it?
9.6 Does the system provide security help based on user expertise (e.g. novice or expert)?
10. Identity Signal – the system should use and display information about validated certificates
10.1 Does the system notify the users when they are interacting with non-trustworthy sources (non-trustworthy is a source that has no information about its identity)?
10.2 Is the information displayed in the identity signal derived from validated certificates?
11. Security and Privacy – the system needs to ensure integrity, availability, confidentiality and privacy
11.1 Does access to protected or confidential areas require authenticators?
11.2 Is it clear that the users give consent regarding the use of their personal information?
11.3 Is it clearly stated for what purposes users' personal information is used?
11.4 Can the user update or delete inaccurate personal information?
11.5 In the case where the user must provide sensitive personal information, does the system state what measures are used to protect this data and ensure that these are taken?
11.6 Does the system enforce a limit of consecutive invalid access attempts by a user during a period of time?
11.7 Are notification messages relating to security and privacy displayed to the user before access to the system is granted (e.g. please log-off your account during lunch time)?
11.8 Are there controls in place that will assist the user in making sharing/collaboration decisions?
11.9 Does the system ensure that publicly accessible information does not contain non-public information?
11.10 Does the system provide notification to the user upon discovering discrepancies during integrity

verification?
11.11 Does the system notify the user about the procedure to be followed in the case of duplication or loss of personal information?
11.12 Does the system employ mechanisms to assist in the reporting of security incidents?
11.13 Does the system notify the user of any information system weaknesses or vulnerabilities associated with reported security incidents?
11.14 Does the system provide a contact for the users' security-related questions?
11.15 Is there a backup policy that regulates how copies of information are taken?
11.16 Does the system enforce minimum password complexity?
11.17 Does the system encrypt passwords in storage and in transmission?
11.18 Does the system prohibit password reuse for a defined number of cycles?
11.19 Does the system employ cryptographic mechanisms to prevent unauthorised disclosure of information during transmission?
11.20 Does the system require users to confirm statements indicating that they understand the conditions of access and are these explicated so that informed decisions can be made (e.g. do you accept that "cookies" are recorded upon registration: cookies track your online browsing activities)?

8.6 TRIANGULATION OF RESULTS

Section 5.7 discussed triangulation, where it was mentioned that this study will use triangulation to enhance the credibility of the findings through the application of several data collection and analysis techniques. From a data collection perspective, those that were applied in this study included a literature review, FUE, user satisfaction questionnaires and HE. From a data analysis perspective, those that were applied include descriptive statistics and theme analysis.

A concept map for this research study is presented in figure 8.14. The map presents the main research question with its supporting sub-questions. The research philosophy adopted for this study was interpretivism and the research strategy applied is a case study. To answer sub-question 1, the fields of HCI, InfoSec and USec had to be investigated. The data collection technique considered for this was a literature study. To answer sub-question 2, a more in-depth investigation into the HE UIM was required. Again, the technique considered for this was a literature study. To answer sub-question 3, an investigation of the assessment criteria was required. Research techniques applied include FUE, HE and user satisfaction questionnaires. To answer sub-question 4, supporting instruments for developing a framework were investigated. Once all the data from the various techniques were collected they were analysed using theme analysis and descriptive statistics, as were discussed in sections 5.3.7.1 and 5.3.7.2 respectively. The outcome of the triangulation process contributes to addressing the main research question. In order to understand how data triangulation was conducted, a data triangulation chart for this research study is also provided in table 8.3.

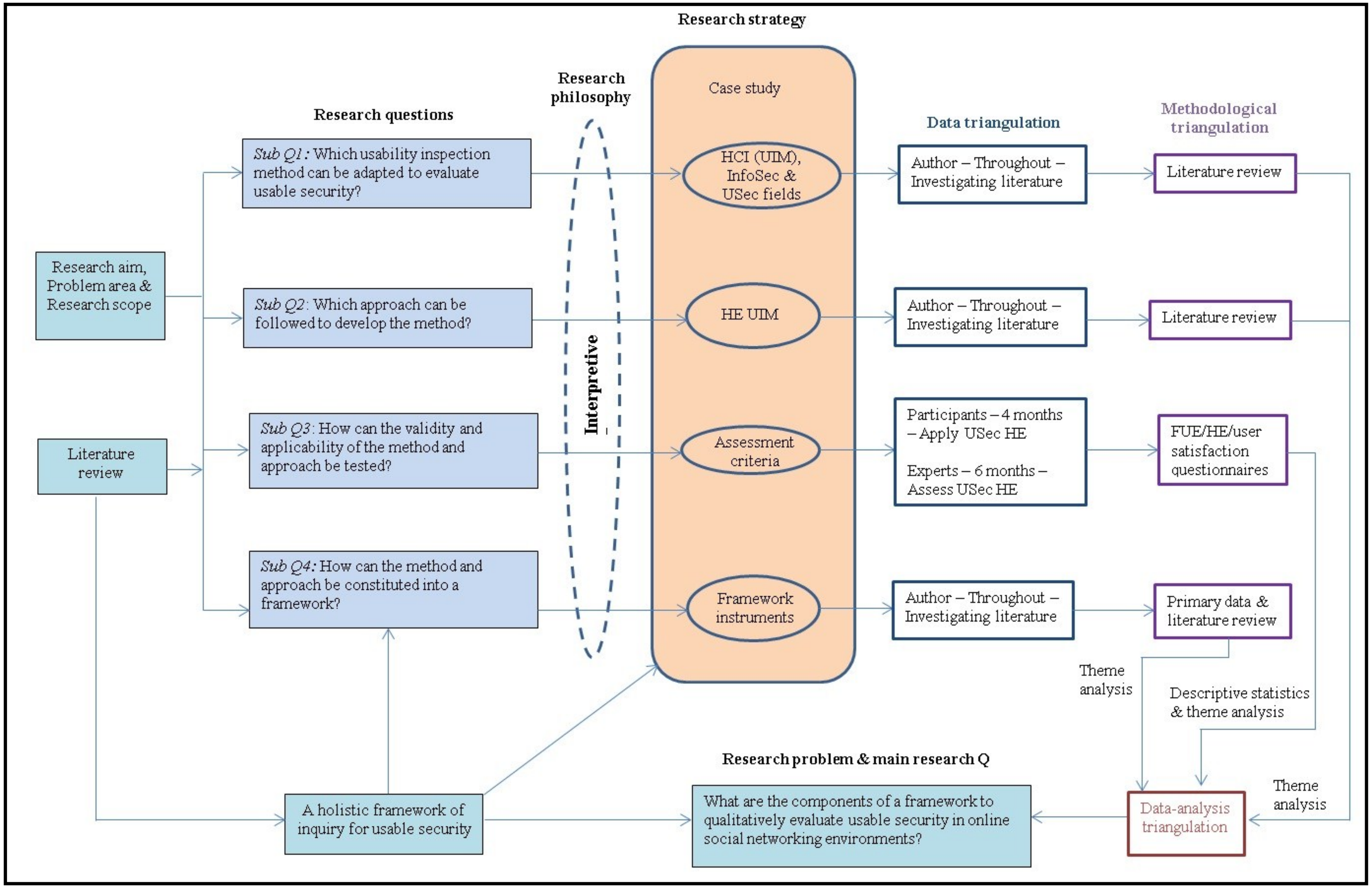

Research strategy
Research philosophy
Case study
Research questions
Data triangulation
Methodological triangulation
Sub Q1: Which usability inspection method can be adapted to evaluate usable security?
HCI (UIM), InfoSec & USec fields
Author – Throughout – Investigating literature
Literature review
Research aim, Problem area & Research scope
Sub Q2: Which approach can be followed to develop the method?
HE UIM
Author – Throughout – Investigating literature
Literature review
Interpretive
Literature review
Sub Q3: How can the validity and applicability of the method and approach be tested?
Assessment criteria
Participants – 4 months – Apply USec HE
Experts – 6 months – Assess USec HE
FUE/HE/user satisfaction questionnaires
Sub Q4: How can the method and approach be constituted into a framework?
Framework instruments
Author – Throughout – Investigating literature
Primary data & literature review
Theme analysis
Descriptive statistics & theme analysis
Research problem & main research Q
Theme analysis
A holistic framework of inquiry for usable security
What are the components of a framework to qualitatively evaluate usable security in online social networking environments?
Data-analysis triangulation

Figure 8.14: The concept map for this research study (based on: Alqatawna, Siddiqi, Akhgar, & Btoush, 2009)

The data triangulation chart displays the data collection techniques that were used to collect the data and interprets the way in which each of them relates to a specific goal. The techniques supported the main research strategy, which was a case study.

Table 8.3: The data triangulation chart for this study

Source number	1	2	3	4
Data techniques & procedures	Literature review or secondary data	FUE	User satisfaction questionnaires	HE
Objective	Gather the required background knowledge in the related fields (OHSNs, research methodology, InfoSec, HCI, and USec).	Provide users with scenarios and tasks to perform on OHSNs.	Gather users and experts opinions about the USec HE.	Users will use the USec HE to evaluate the OHSNs. Experts will use a validation tool to assess the USec HE.
Interpretation (results)	• Understand the purpose of USec for OHSN (Source 1). • Understand UX and its role in design (Source 1). • Understand the requirements for InfoSec (Source 1). • Select the appropriate research methods for the study (Source 1). • Select the appropriate UIM for evaluating USec (Source 1). • Determine how to create a USec HE (Source 1). • Determine the difficulties and frustrations of users when interacting with security and privacy on an OHSN (Source 2). • Determine the users' preferences, regarding security and privacy on an OHSN (Source 2). • Determine the level of USec on the two OHSNs (Source 2). • Determine the users' overall perceptions of the OHSNs (Source 3). • Determine the users' and experts perceptions about the use and application of the USec HE (Source 3). • Evaluate the OHSNs with the USec HE (Source 4). • Evaluate the USec HE (Source 4).			

The overall findings from the data triangulation chart support the validity and credibility of the three components of the framework. These include the process to develop heuristics for SADs, the validation tool and the USec HE, which all form part of the framework to evaluate USec in social networking environments.

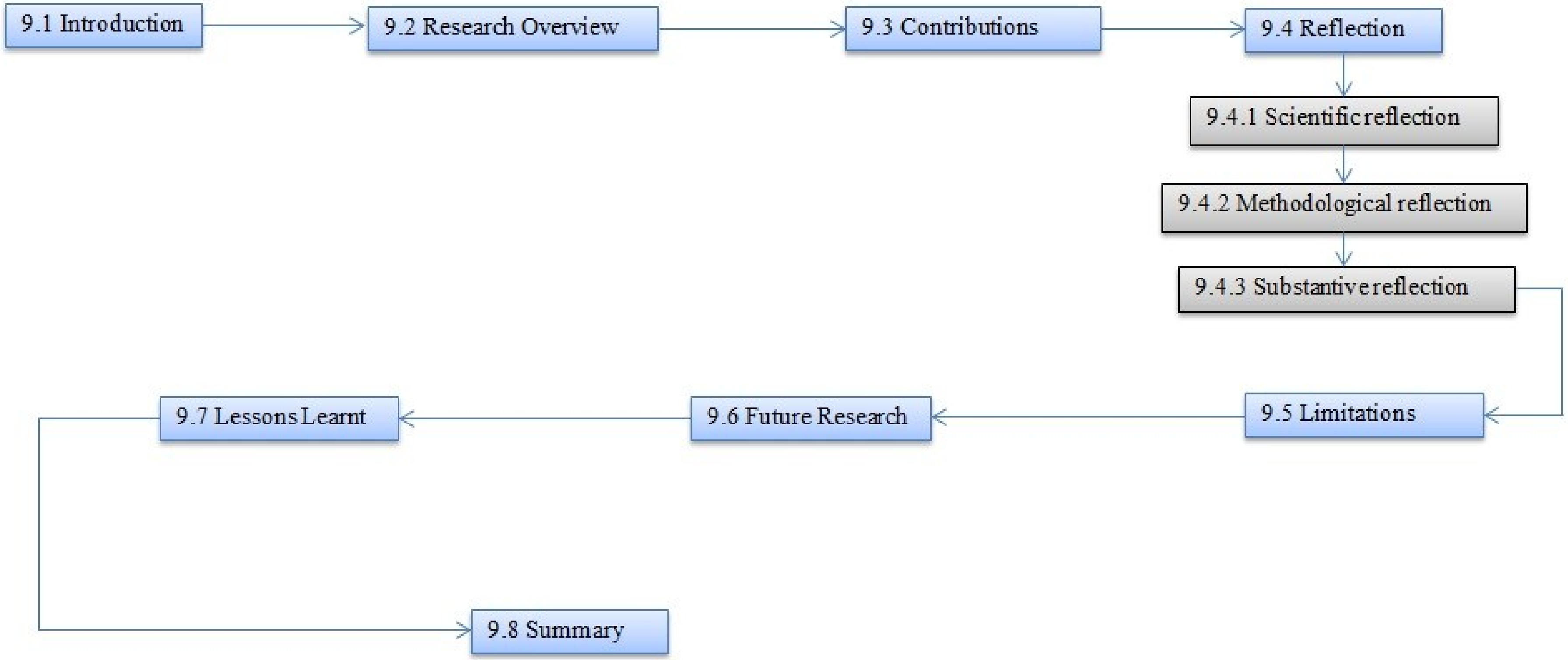
8.7 SUMMARY

This chapter presented a framework to evaluate USec in online social networking environments. Based on the review of frameworks in section 5.5, the framework for this study was defined. There were seven instrumental steps in its formulation, while the relationships and outputs of its components were acknowledged. The three components are the process to develop heuristics for SADs, the validation tool and the USec HE. Each was discussed in its own section.

The first component, the process to develop heuristics for SADs, was then briefly discussed. The discussion focused on how the process was applied to develop USec heuristics and presented the tasks that were conducted in each phase. Following this was a discussion on the second component, the validation tool, during which the seven sheets of the tool were presented. Once again, reference was made to how the sheets were applied to assess the USec HE. Subsequently, the third component, the USec HE was discussed. The modified heuristics and their checklist items were presented in this section.

The chapter ended with a view of the data triangulation chart for this study. It mentioned the four data techniques and procedures that were used and presented their goals, which are the product of the triangulation process. The results indicate the validity and credibility of the framework's components. In chapter 9, the conclusion of the research study will be presented.

LAYOUT OF CHAPTER 9



CHAPTER 9: CONCLUSION

9.1 INTRODUCTION

The purpose of this research study was to develop a framework for evaluating USec in online social networking environments. The first gap identified in the literature was a lack of tools for evaluating USec, while the second and third gaps identified were the lack of a process to develop heuristics and, subsequently, to validate them, respectively. OHSNs provided an applicable context in which to evaluate the solutions to the identified gaps. This final chapter provides a platform for summarising the entire research study.

Section 9.2 will provide an overview of the research and the contributions made by the research are discussed in section 9.3. Section 9.4 provides a reflection of the research from several perspectives and section 9.5 discusses the limitations of the study. Areas for future research are identified in section 9.6. The lessons learnt from this research experience are presented in section 9.7. The final section, section 9.8, comprises a summary.

9.2 RESEARCH OVERVIEW

The research commenced by reviewing the existing body of knowledge and the review was discussed in chapters 2 and 3. In particular, chapter 2 discussed the field of HCI and its disciplines that are of relevance to this study. These included UCD, HCD, usability and UX. The chapter also mentioned the UIMs that are commonly applied in the field, with more emphasis on HE. In chapter 3, USec was discussed. In this chapter, InfoSec and privacy were introduced first and an outline of the USec field was complemented with a discussion on current evaluation tools. These include guidelines, standards and practical solutions for USec.

The process for developing heuristics for SADs and the USec heuristics and checklist items is first presented in chapter 4. That chapter demonstrates how the process is based on the HCD approach and then presents all three phases of the process in detail. This is followed by a detailed discussion on how the heuristics and checklist items for USec were developed.

The research design and methodology is presented in chapter 5. The research onion model was used to explain the methodology, of which more detail is provided later in this section. Data collection and analysis techniques, frameworks and data triangulation are also introduced in this chapter.

Chapter 6 provides an exploration of OHSNs. This included capabilities and barriers, among other information. Subsequently, the case study concerning MedHelp and Google Health was discussed. The participants and the scenarios and tasks they performed in the FUE were mentioned. Participants then applied the USec HE in order to evaluate the OHSNs and completed a user satisfaction questionnaire. The results of the analysis were presented and discussed and on this basis recommendations for USec were made for each OHSN. Participants also provided feedback for improving the USec HE.

The assessments that experts conducted on the USec HE were discussed in chapter 7. Accordingly, experts applied the validation tool, consisting of seven sheets and on the basis of results and analysis of these assessments; it was possible to make improvements to the USec HE. The reasoning for implementing the suggested improvements to the USec HE is documented in the chapter.

In chapter 8, the framework for evaluating USec in online social networking environments is presented. Its three components comprise the process to develop heuristics for SADs, the validation tool and the USec HE. These represent the modified heuristics and checklist items for USec, based on the improvements suggested in chapter 7, as well as the results of a second iteration of the process. These contributions will be discussed again in section 9.3. The data triangulation process was then reviewed.

Founded on the problem description and rationale in chapter 1, a primary research question and supporting sub-questions were derived. The primary research question for this study is the following:

What are the components of a framework to qualitatively evaluate usable security?

The sub-questions are:

1. *Which usability inspection method can be adapted to evaluate usable security?*
2. *Which approach can be followed to develop the method?*
3. *How can the validity and applicability of the method and approach be tested?*
4. *How can the method and approach be constituted into a framework?*

The research design and methodology were critical in answering the primary and sub-questions. To reiterate, the research onion model was used as a platform. Based on the model, this study identified the following components of the research methodology:

- An interpretivist research philosophy
- An inductive reasoning research approach
- A case study research strategy
- A mixed-methods choice
- A longitudinal time horizon
- Four techniques and procedures – secondary data, questionnaires, HE and FUE. These are supported with data triangulation.

The four sub-questions were answered in different sections of the thesis. Table 9.1 summarises the answers to all the research questions and presents a brief overview of their solutions. The sections in the thesis where each of the questions were referenced is also provided. It should be noted that a particular sub-question may be referenced in more than one section. From the table, it can be concluded that all sub-questions have been addressed. Accordingly, the primary research question has also been answered.

Table 9.1: Addressing the primary and sub-questions of the research study

Research Question	Type	Answer	Overview	Reference
What are the components of a framework to qualitatively evaluate usable security?	Primary	• Process to develop heuristics for SADs • Validation tool • USec HE	By addressing the sub-questions, a framework for evaluating USec in social networking environments was constructed and presented in chapter 8.	Section 8.2
Which usability inspection method can be adapted to evaluate usable security?	Sub	HE	The HE UIM is discussed in general in chapter 2. The USec HE specifically, is presented in chapter 4.	Sections 2.6.9 4.4.
Which approach can be followed to develop the method?	Sub	Process to develop heuristics for SADs	The literature considered for developing the process is presented in chapter 2. The three-phase process is presented in chapter 4.	Sections 2.6.9 4.3
How can the validity and applicability of the method and approach be tested?	Sub	Method: • Case study • Validation tool • Publication	Method: • The results from applying the USec HE to evaluate OHSNs are presented in chapter 6.	Method: Section • 6.3.2 6.3.3 • 8.5

Research Question	Type	Answer	Overview	Reference
		Approach: • Case study • Publication	• The results from the validation tool are presented in chapter 7. Based on both of the above, the improved USec HE is presented in chapter 8, while the complete tool with severity ratings is available in *Appendix A.1: USec HE.* • Publication of the method is available in Appendix *E.7: A Usable Security Heuristic Evaluation for the Online Health Social Networking Paradigm*. Approach: • The results from applying the process to develop a USec HE are presented in chapter 8. • Publication of the approach is available in Appendix *E.5: A Three-Phase Process to Develop Heuristics*.	Approach: • 8.3
How can the method and approach be constituted into a framework?	Sub	Define supporting instruments: • 3 components • 3 relationships • 5 outputs • Context	The supporting instruments were discussed in chapter 8. These provide the foundations for answering the main research question.	Section 8.2

9.3 CONTRIBUTIONS

The importance and impact of USec is stressed throughout the thesis. Although many within the research community share this view, as was mentioned in chapter 3, it is not supported by all. In alignment with the notion that USec is beneficial, particularly in social networking environments, a direction for this research was formulated. This research study spanned the period from 2009 to 2011 and aimed at investigating the design of a framework for evaluating USec in social networking environments.

This study has added to the body of knowledge of USec and HCI. In so doing, this study has identified and developed a conceptual framework that outlines the way in which USec can be evaluated in the context of online social networking. The framework clarifies the components and outputs that are influenced by the relationships that exist between the components themselves and the online social networking environment. Therefore, it can be noted that this study contributes to evaluating USec in online social networking environments, especially in a health context.

The study is also unique as the framework incorporates three novel components: a process, a validation tool and an HE, which were all developed in this research as well:

- *Process to develop heuristics for SAD* – This is a three-phase process that can be followed when developing heuristics for a SAD. In phase 1 high-level heuristics are designed; in phase 2, the high-level heuristics are validated and in phase 3, the high-level heuristics are applied in a context. This process adds to the body of knowledge for HCI because it focuses on developing new HEs, which are the most frequently used UIM.
- *Validation tool* – The validation tool is applied to assess the new high-level heuristics and checklist items for a SAD. This occurs in phase 2 of the process. The validation tool comprises seven sheets: instructions, expert biographical information, heuristics assessment, checklist items assessment, severity ratings, material assessment and satisfaction questionnaire. The tool forms a template that can be customised specifically for the assessment of heuristics for a SAD.
- *USec HE* – This is an HE that is specific to the application domain of USec and is used to identify USec violations on an interface of a website/application. As a result it is possible to determine the severity of these violations and to recognise where improvements are necessary.

From a practical perspective, the study led to the development of two reliable measuring instruments in the validation tool and the USec HE. Beyond the boundaries of the framework, these can be considered as contributions in their own right. The HE can be used to measure the level of USec on websites/applications and the validation tool can be used to assess a new set of heuristics and checklist items for a SAD. With adjustments, the validation tool may be applicable for assessing an HE for a SAD.

The USec HE was applied to evaluate two OHSNs. However, prior to its use, two additional contributions were made:

- *Requirements for OHSNs* – These can be used to define an OHSN. There are four sets of requirements and each has its own criteria: social networking components, health application domain, scope of functionality and supplementary factors. The criteria for the social networking components are profile, connections, navigation, multiple means of connections, visibility controls, tools for interaction and access controls. The criteria for the health application domain are free-standing vs. integrated, patient-specific vs. health-care provider specific and general health vs. disease-specific. The criteria for the scope of functionality are end-user participation empowerment, medical education and information and trustworthiness. The criteria for the supplementary factors are number of users, number of support groups and brand.

- *USec recommendations for MedHelp and Google Health* – The case study that was conducted on the two OHSNs yielded a number of USec recommendations. For MedHelp there were a total of 41 recommendations: thirteen for trust, four for ease of use, four for terminology, four for ease of learning, six for feedback, six for awareness, two for errors and two for help and documentation. For Google Health there were a total of 22 USec recommendations: six for trust, three for terminology, two for ease of learning, three for feedback, four for awareness, three for errors and one for help and documentation. These are defined as practical contributions.

The recommendations for improving USec on MedHelp and Google Health support the notion that security and privacy impact on UX as well. In chapter 2, the UX Honeycomb was introduced. To reiterate, this currently consists of seven facets for UX: useful, usable, desirable, findable, accessible, credible and valuable. Morville (2004) suggests that new facets be introduced to further develop the UX Honeycomb. Considering this in alignment with the view that security and privacy impact UX, the research supports the recommendation stated earlier in chapter 2 to include an eighth facet; the “secure” facet; into the UX Honeycomb to complement the existing seven facets. The Secure facet will be concerned with the users’ ability to perform security actions and to protect their personal information easily and effectively when interacting with the security and privacy features of an application/website.

The verification of the contributions in this research study is exemplified by the scientific publications emanating from it, which currently include the thesis and four publications.

Following the above discussion, it is clear that the results of this research study offer relevant, scientific and practical contributions, as well as recommendations and suggestions.

9.4 REFLECTION

In this section reflections are provided from three perspectives; scientific, methodological and substantive.

9.4.1 Scientific Reflection

The problems that users experience with security and privacy were discussed in chapter 3. The fact that security is a problem area for UI design also contributes to poor USec. Consequently, developers require tools that can assist them to improve their designs in terms of USec. Security and privacy design issues can be alleviated with the USec HE. This is a contribution to the USec field.

The problems with designing heuristics have been discussed in chapter 2. The fact that well-known heuristic sets can be limited in scope when evaluating a SAD contributes to inferior evaluation results. HCI researchers require a process in which new HEs can be developed. In addition, new HEs also need to be assessed for their validity. The process to develop heuristics for SADs and the validation tool are therefore contributions to the HCI field.

The problems that users face in OHSNs have been discussed in chapter 6. All online social networking environments share these, as they are not specific to health only. However, those for health do have particular added concerns. Accordingly, users require usable features that can assist them in best protecting their personal information in such environments. The framework to evaluate USec in online social networking environments is therefore a contribution to the field of USec, HCI and online social networking.

9.4.2 Methodological Reflection

This study investigated elements from the fields of HCI and InfoSec. The methodologies used in HCI are more qualitative than those for InfoSec, owing to the investigation of human behaviours. This requires the researcher to analyse and interpret results in specific contexts. Thus, it is more difficult to generalise results when conducting HCI research than InfoSec.

Conducting research in the field of USec can be challenging and requires the researcher to have an understanding of both the HCI and InfoSec fields, which often conflict with each other in terms of their methodologies and objectives. It is even more challenging for researchers to be neutral and unbiased towards their own research background. Initially one would expect the researcher to remain neutral in the research process. However, one subsequently realises that the researcher has to have a stance, as this represents the point of departure for the research. This is the approach that was taken for this study – point of departure is an HCI perspective. However, it is still important to be unbiased and to consider the field of InfoSec separately. If not, the research will not adequately represent the InfoSec field, which in turn will not embody the field of USec.

The methodologies used in this research are more qualitative in nature, owing to the research stance that was taken. Nonetheless, quantitative data were collected from the user satisfaction questionnaires of the participants and the experts. These were analysed in terms of frequency counts so that conclusions could be derived from the results. Besides the literature review that was conducted for the InfoSec field, the validation tool also ensures that InfoSec is represented appropriately in the design of the USec HE. Moreover, the comments and assessments of the InfoSec and USec experts guarantee this.

9.4.3 Substantive Reflection

Reflecting on this study, it can be recognised that the scope for research in the field of USec is wide, as it encompasses two fields; HCI and InfoSec. Determining the point of departure for the research study is a priority and this is done by taking a stance. With regards to this study, the scope was also deemed wide, as it focused on multiple aspects, which make the contributions unique. Accordingly, the research required the following:

- An understanding of the fields of HCI, InfoSec and USec to develop a USec HE
- An understanding of UIMs to determine how to develop heuristics and checklist items
- An understanding of evaluation criteria and Likert scales for the design of attitude instruments to determine how to validate a new HE
- An understanding of social networking environments to determine requirements for selecting OHSNs

The USec HE is a tool that will benefit users and developers alike. Developers can have their security and privacy features evaluated to ensure that they are usable. By doing so, users will be provided with security and privacy features that they can use and understand on their respective websites/applications. It is possible however, that the USec HE may need to be upgraded owing to technology changes. New technologies for security and privacy may require new heuristics and checklist items to evaluate them, if the existing ones are deemed inefficient.

9.5 LIMITATIONS

Reflecting on the research study, the following limitations became apparent:

- The FUE were conducted with postgraduate students that had no experience with OHSNs. Preferably, one would have used participants who are registered on an OHSN to conduct the evaluations. Participant selection was discussed in section 6.3.1.2.
- The validation tool was conducted by two experts from InfoSec, one from HCI and one from USec. In terms of conducting an HE, this number is adequate, as the literature states that three to five evaluators are recommended. However, more experts, particularly from the USec field, may have contributed to a higher quality and more effective USec HE. Nonetheless, identifying USec experts is challenging, as they are restricted in numbers.
- The length of the validation tool minimised the response rate from the experts. This is discussed in more detail in section 9.6 because it also offers an area for possible future research.
- The case study was conducted in the context of OHSNs. Within this context, the case study is applicable because it evaluates two cases. However, it would be valuable to conduct a case study in a different context as well (e.g. evaluate the level of USec in the context of e-banking). This is elaborated on more in section 9.6 because it also offers an area for possible future research.
- Requirements that define an OHSN do not exist. Therefore, these had to be established in this research study by reviewing the relevant literature and by interacting with such websites. Once these were established, the author applied them to determine the two OHSNs that would be used in the case study. The selection process was conducted by the author alone, who also established the requirements.

9.6 FUTURE RESEARCH

Within the various chapters, areas for possible future research were identified. These are mentioned again below. In addition to these, other areas are also identified. The areas for possible future research include:

- *Applying the USec HE to evaluate another website/application* (e.g. Facebook, MS Outlook, e-banking websites etc.). This provides a new context in which to evaluate USec. Based on the results of the user satisfaction questionnaires that participants completed, the quality and effectiveness of the USec HE was regarded as more than satisfactory. However, it would seem there is still room for improvement. By applying the USec HE in another context, its effectiveness can be further exemplified. Together, areas that the USec HE fails to evaluate for a specific context can be determined and improvements subsequently made to them. This will further improve the quality of the USec HE, because it considers areas that are context specific. These can be regarded as "optional heuristics and checklist items". Therefore, if they do not apply in a different context, they are simply not used.

- *Developing heuristics for a different SAD* (e.g. heuristics to evaluate the design of instructional e-learning websites for the Deaf). In this example the SAD is an instructional e-learning websites for deaf users. Therefore, the literature review would focus on the design of instructional e-learning websites and on the abilities and preferences of deaf users when interacting with websites. In essence, the aim is to follow the three-phase process in order to create heuristics for another SAD. Areas where the process can be improved or modified may then be identified. By creating a second set of heuristics, the applicability of the process is further substantiated.
- *Improving the validation tool from the expert perspective*. Based on the experts' comments, the main concern with the validation tool was its length. Experts suggested that it would be useful to provide an alternative shorter version of the tool. This was also the reason that only four of the seven experts returned their assessments by the cut-off date. However, the USec expert also mentioned that the tool provided interesting and relevant ideas. In addition, the expert liked the approach applied in the validation. It is possible that when using the validation tool for a different SAD it could be shorter in length. For the USec SAD it was extensive in order to ensure that the HCI and InfoSec fields were well represented. As mentioned previously, the validation tool is a template that can be customised. For example, if a new set of heuristics for a SAD are not supported with checklist items, the checklist items assessment sheet could be excluded from the tool. Or, if no customised severity ratings are required for the SAD, the severity ratings sheet could be excluded. It is worthwhile investigating how the validation tool can be improved for the experts, as it is already regarded as an effective tool. Therefore, improvements would be focused on enhancing the experience that experts have when using the tool. For example, if they are concerned with the length of the tool, it may impact negatively on their

assessments even before they start using them. Enhancing their experience will contribute to the provision of optimal assessments.

- *UI design implementations for USec*. Practical implementations for USec are still limited. Expanding on the existing solutions, heuristics or checklist items from the USec HE may be formed into ideas for UI design implementations. The user suitability heuristic is a worthy example. It states that the system should consider the diverse skills of users when providing them with security related information. Thus, a new UI design implementation for USec could monitor the users' interactions with the security and privacy features in an attempt to determine their level of skill. Once this has been determined, security information and settings can be presented in a manner that suits their skill level. Nonetheless, users should still have the option to select their preferred skill level as well.
- *Verification of a website/application security capability claims*. This would focus on how security and privacy claims in policies can be verified. It is important for users to know exactly how their personal information is protected, and user trust can be enhanced by verifying the claims. In terms of OHSNs, this extends beyond valid certificates and codes that verify health information. For example, stating in the policy that weekly backups are made should be verified to guarantee that this actually does happen.
- *Designing more usable online policies*. This is an area that is well researched and that has a direct impact on USec. For example, Patrick and Kenny (2003) considered four categories of human factor requirements for effective privacy interface design. Based on these, they developed a technique to demonstrate how interface design solutions can be used when developing a privacy-enhanced application or service. This is just one idea for designing more usable privacy solutions. In support of this, in the validations conducted, an InfoSec expert expressed the opinion that users should not be confronted with a blanket accept-or-deny situation for a complete policy. Rather, the policy should be more individualised. For example, in terms of an OHSN, users should be able to select which personal information they give consent to be utilised by the OHSN and other third-party websites.

9.7 LESSONS LEARNT

It is valuable to mention additional lessons that were learnt during the course of this research study, as they make for interesting reading and in principle support the work conducted in this research.

The participants who conducted the FUE were unaware of the field of USec, despite the fact that their research backgrounds are in the fields of HCI, InfoSec and Health Informatics. Understandably, this would be expected considering that HCI and InfoSec have opposing objectives. Nevertheless, by the time they completed their evaluations, they all appreciated the significance of developing USec tools. This view is confirmed in the results of their user satisfaction questionnaires.

The experts who assessed the USec HE with the validation tool presented similar views to those of the participants. They also realise the difficulties that users experience with security and, therefore, their views express a need for more USec tools. This is aided by their support for the development of a USec HE. Their feedback was essential to improving the USec HE and in delivering a tool that should satisfy advocates from the HCI, InfoSec and USec fields. Experts found this type of research very interesting and all look forward to the analysis of the results. The fact that seven experts initially accepted the invitation to participate is also testament to this; this despite the fact that three of those experts could not complete their validations. This was a result of the length of the validation tool and their other commitments.

The inferences made are that the field of USec is still young and provides opportunities for ample research. This study shows that this type of research is equally necessary and interesting. Most important of all, it proved that researchers from the fields of HCI and InfoSec are willing to contribute and work together to provide USec research and solutions. This was observed in the positive attitudes and feedback provided by both the postgraduate students and the experts.

Based on this experience, the paradox that exists in USec is questioned. Claims that usability and security cannot be merged have been proven invalid in this case. Instead of allowing such a view to persist, it is proposed to rather abandon it and to concentrate efforts on collaboration. Accordingly, this research demonstrates the outcomes of collaboration. Without the collaboration of researchers and experts in the fields of HCI, InfoSec, USec and Health informatics, success in this research would have been jeopardised. The researcher maintains that research in USec cannot be conducted in any other fashion; by following this approach, the belief is that a beneficial tool for USec has been developed.

9.8 SUMMARY

This chapter summarises the research study. Following the introduction, a research overview was presented in section 9.2, which outlined the discussions that were undertaken in each chapter and presented the primary research question and sub-questions of the study. How and where these are addressed in the thesis was also mentioned. Section 9.3 emphasises the unique contributions made by this research study.

Reflections from scientific, methodological and substantive perspectives are provided in section 9.4. The scientific reflection generalised several contributions in the context of the research community, while the methodological reflection described the stance taken to conduct USec research and, finally, the substantive reflection defined the scope of the study.

In section 9.5, the limitations of the research study were listed, some of which provide opportunities for future research. These and other areas for possible future research are discussed in section 9.6. Arising from this research, six areas for future research were identified. In conclusion, section 9.7 pointed out some of the lessons that were learnt during the course of this research study. Based on the experience gained, these lessons were subtly transformed into suggestions for conducting USec research.

LIST OF REFERENCES

A

Ackerman, M. & Mainwaring, S. (2005). Privacy issues in human-computer interaction. In L. Cranor & S. Garfinkel (Eds.) *Security and usability: Designing secure systems that people can use*. Sebastopol, CA: O'Reilly, pp 381–400.

AICPA. (2005). *Comparison of international privacy concepts*. Retrieved September 14, 2009 from the World Wide Web: http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/GenerallyAcceptedPrivacyPrinciples/GenerallyAcceptedPrivacyPrinciplesAppendixes/Pages/Appendix%20B%20Comparison%20of%20International%20Privacy%20Concepts.aspx

AICPA. (2009). *Privacy: An introduction to generally accepted privacy principles*. Retrieved September 14, 2009 from the World Wide Web: http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/GenerallyAcceptedPrivacyPrinciples/Pages/Privacy%20%20An%20Introduction%20to%20Generally%20Accepted%20Privacy%20Principles_Oct1909_Jan1510_%20BT_Update.aspx

Alder, K.G. (2006). Web portals in primary care: An evaluation of patient readiness and willingness to pay for online services. *Journal of Medical Internet Research*, 8(4): e26. DOI: 10.2196/jmir.8.4.e26.

Alqatawna, J., Siddiqi, J., Akhgar, B. & Btoush, M.H. (2009). E-business security: Methodological considerations. *World Academy of Science, Engineering and Technology,* January vol. 49: 624. Dubai, United Arab Emirates. ISSN: 2070-3724.

Ardito, C., Costabile, M., Lanzilotti, R. & Montinaro, F. (2007). Towards the evaluation of UX. Workshop "Towards a UX Manifesto" at the International Conference HCI 2007, Lancaster, UK, September 3, pp. 6–9.

B

Babbie, E. & Mouton, J. (2001). *The practice of social research*. Cape Town: Oxford University Press.

Babbie, E. R. (2005). *The basics of social research*. Third edition. Belmont, CA: Wadsworth Publishing.

Baker, W., Goudie, M. & Hylender, C. D. (2010). *Verizon 2010 Data Breach Investigations Report*. Methodology, 65. Retrieved February 18, 2011, from the World Wide Web: www.verizonbusiness.com/go/2010databreachreport/

Baker, K., Greenberg, S. & Gutwin, C. (2001). Heuristic evaluation of groupware based on the mechanics of collaboration. In: *Proceedings of the 8th IFIP International Conference on Engineering for Human-Computer Interaction*, May, pp. 123–140.

Balfanz, D., Durfee, G.E., Smetters, D.K. & Grinter, R.E. (2004). In search of usable security - Five lessons from the field. *IEEE Security & Privacy Journal*, 2(5): 19–24.

Ballard, J.K. (2010). Web site usability: A case study of student perceptions of educational Web sites. PhD dissertation, University of Minnesota.

Barnum, C.M. (2002). *Usability testing and research*. New York, NY: Longman.

Benyon, D., Turner, P. & Turner, S. (2005). *Designing interactive systems: people, activities, contexts, technologies*. Harlow, England, New York: Addison-Wesley.

Bernardo, T. (2005). A model for information architecture of government websites in Southern Africa. MSC Dissertation, NMMU. Port Elizabeth.

Bhattacherjee, A. (2011). *Social science research: principles, methods, and practices*. Second edition. Tampa, Florida: University of South Florida.

BoK-a (2005). *Usability body of knowledge: Usability engineering*. Retrieved December 19, 2009, from the World Wide Web: http://www.usabilitybok.org/glossary

BoK-b (2005). *Usability body of knowledge: User-centred design*. Retrieved December 19, 2009, from the World Wide Web: http://www.usabilitybok.org/glossary

BoK-c (2005). *Usability body of knowledge: Testing (usability).* Retrieved December 19, 2009, from the World Wide Web: http://www.usabilitybok.org/glossary

Borland, J. (2007). A smarter Web (1099274X). *Technology Review*, 110(2): 64–71. From Academic Search Premier Database.

Boulos, M.N.K. & Wheelert, S. (2007). The emerging Web 2.0 social software: an enabling suite of sociable technologies in health and health care education. *Health Information and Libraries Journal,* 24(1): 2–23.

Boyd, D.M. & Ellison, N.B. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, 13(1), article 11. Retrieved August 04, 2009 from the World Wide Web:
http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html

Brunk, B. (2005). A user-centric privacy space framework. In: Cranor, L.F. & Garfinkel, S. (Eds.). *Security and usability: Designing secure systems that people can use*. Sebastopol, CA: O' Reilly Media Inc., pp 401–420.

Brustoloni, J.C. (2005). Hardening Web browsers against man-in-the-middle and eavesdropping attacks (with H. Xia). In *Proceedings of the 14th International World Wide Web Conference (WWW2005),* ACM, Chiba, Japan, pp. 489-498, May 2005.

Butler, M.B. (1996). Getting to know your users: usability roundtables at Lotus Development. *Interactions*, Jan 3(1): 23–30.

Butow, E. (2007). *User interface design for mere mortals*. Boston, Mass Addison-Wesley.

C

Carroll, J.M. (2003). *HCI models, theories, and frameworks: Towards a multidisciplinary science.* San Francisco, CA: Morgan Kaufmann.

Centre for Democracy and Technology. (2009). *CDT's guide to online privacy. Privacy Basics: The OECD Guidelines, 2009.* Retrieved September 10, 2009 from the World Wide Web: http://www.cdt.org/privacy/guide/basic/oecdguidelines.php

Chiasson, S., Forget, A., Biddle R. & Van Oorschot, P.C. (2008). *User interface design affects security: Patterns in click-based graphical passwords.* Technical Report TR-08-14, School of Computer Science, Carleton University.

Clark, L. & Sasse, M.A. (1997). Conceptual design reconsidered: The case of the Internet session directory tool. In *Proceedings of HCI'97* in Bristol, August 12–15. Springer.

Cockton, G. & Woolrych, A. (2001). Understanding inspection methods: Lessons from an assessment of heuristic evaluation. In: Blandford, A. & Vanderdonckt, J. (Eds.), *People & computers XV.* Springer-Verlag, pp 171–192.

Cockton, G. & Woolrych, A. (2002). Sale must end: Should discount methods be cleared off HCI's shelves? *Interactions*, 9(5): 13–18.

Cranor, L. (2005). Privacy policies and privacy preferences. In: Cranor, L.F. & Garfinkel, S. (Eds.). *Security and usability: Designing secure systems that people can use*. Sebastopol, CA: O'Reilly Media, pp 447–472.

Creswell, J.W. (2004). Educational research: Planning, conducting, and evaluating quantitative and qualitative research. Second edition. Upper Saddle River, N.J: Prentice Hall.

Creswell, J.W. (2009). Research design: Qualitative, quantitative, and mixed methods approaches. Third edition. Thousand Oaks, CA: Sage.

D

De Villiers, M.R. (2005). Three approaches as pillars for interpretive information systems research: development research, action research and grounded theory. Proceedings of the 2005 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries. White River, South Africa, pp. 142–151.

Denzin, N.K. (1970). *The research act: A theoretical introduction to sociological methods*. Chicago: Aldine.

DeVaus, D.A. (2002). *Surveys in social research*. Fifth edition. London: Routledge.

DiGioia, P. & Dourish, P. 2005. Social navigation as a model for usable security. In Proceedings of the 2005 Symposium on Usable Privacy and Security (Pittsburgh, Pennsylvania, July 6–8,). SOUPS '05, vol. 93. ACM, New York, NY, 101–108. DOI: http://doi.acm.org/10.1145/1073001.1073011

Dix, A., Finlay, J., Abowd, G. & Beale, R. (2004). *Human-Computer Interaction*. Third edition. Harlow, Essex: Pearson Education.

Driscoll, D.L. (2006). *The writing lab & the OWL at Purdue and Purdue University: Analyzing your primary data.* Retrieved July 16, 2009, from the World Wide Web: owl.english.purdue.edu/owl/resource/559/09/

E

Edwards, A.D.N. & Petrie, H. (2005). Memorability and security of passwords. *Interfaces 65,* (Winter): pp. 12–13.

Eysenbach, G. (2008). Medicine 2.0: Social networking, collaboration, participation, apomediation, and openness. *Journal of Medical Internet Research*, 10(3): e22. DOI: 10.2196/jmir.1030.

F

Facebook. (2011). *Statistics*. Retrieved November 18, 2011, from the World Wide Web: http://www.facebook.com/press/info.php?statistics

Farzanfar, R., Finkelstein, J. & Friedman, R.H. (April, 2004). Testing the usability of two home-based patient-management systems. *Journal of Medical Systems*, 28(2): 143–153. DOI: 10.1023/B:JOMS.0000023297.50379.3c

FIPS PUB 199. (2004). Federal information processing standards publication: Standards for security categorization of federal information and information systems. Department of Commerce: USA.

Flechais, I. & Sasse, M.A. (2007). Stakeholder involvement, motivation, responsibility, communication: How to design usable security in e-Science. *International Journal of Human Computer Studies*. DOI:10.1016/j.ijhcs.2007.10.002

Ford, G. (2005). Researching the effects of culture on usability. MSc Dissertation, UNISA.

Frost, J.H. & Massagli, M.P. (2008). Social uses of personal health information within PatientsLikeMe, an online patient community: What can happen when patients have access to one another's data. *Journal of Medical Internet Research*, 10(3): e15. DOI: 10.2196/jmir.1053.

Furnell, S. (2004). Using security: Easier said than done. *Computer Fraud & Security*, Vol. 4: 6–10.

Furnell, S. (2005). Why users cannot use security. *Computers & Security*, 24(4): 274–279. DOI: 10.1016/j.cose.2005.04.003

Furnell, S. (2007). Making security usable: Are things improving? *Computers & Security*, 26(6): 434 (10). DOI: http://find.galegroup.com/ips/RedirectAction.do?URL=http%3A%2F%2Fdx.doi.org%2F10.1016/j.cose.2007.06.003

Furnell, S.M., Jusoh, A. & Katsabas D. (2006). The challenges of understanding and using security: A survey of end-users. *Computers & Security*, Vol.25: 27–35. Retrieved 10 March 2009 from http://linkinghub.elsevier.com/retrieve/pii/S0167404805002038

G

Gaffney, G. (2004). *Contextual enquiry: A primer*. Retrieved December 19, 2009, from the World Wide Web: http://articles.sitepoint.com/article/contextual-enquiry-primer

Garrett, J.J. (2000). *The elements of user experience*. Retrieved August 04, 2009 from the World Wide Web: http://www.jjg.net/ia

Gartner. (2008). *Dataquest Insight: Consumers' Value Perception of the Internet (ID: G00156111)*. Retrieved September 15, 2011, from the World Wide Web: http://www.gartner.com/DisplayDocument?ref=g_search&id=639708&subref=simplesearch.

Giustini, D. (2007). Web 3.0 and Medicine. *British Medical Journal*, 335(7633): 1273–1274. DOI: 10.1136/bmj.39428.494236.BE

Glesne, C. & Peshkin, A. (1992). *Becoming qualitative researchers: An introduction*. New York: Longman.

Gotta, M. (2008). Next document: Reference architecture for social network sites. *Collaborative Thinking*. Retrieved May 19, 2010, from the World Wide Web: http://mikeg.typepad.com/perceptions/2008/07/next-document-r.html

Gould, J.D. & Lewis, C. (1985). Design for usability: Key principles and what designers think. *Communications of the ACM*, 3(28): 360–411.

Gulliksen, J., Goransson, B., Boivie, I., Blonkvist, S., Persson, J. & Cajander, Å. (2003). Key principles for user-centred system design. *Behaviour and Information Technology*, Vol. 22: 397–409.

H

Halamka, J.D., Mandl, K.D. & Tang, P.C. (2007). Early experiences with personal health records. *Journal of the American Medical Informatics Association*, 15(1): 1–7. DOI: 10.1197/jamia.M2562.

Harrison, S., Tatar, D. & Sengers, P. (2007). *The three paradigms of HCI*, alt.chi 2007.

Hassenzahl, M. & Tractinsky, N. (2006). User experience: A research agenda. *Behaviour & Information Technology*, March-April 25(2): 91–97.

Henry, S.L. (2007). *Just ask: Integrating accessibility throughout design*. Madison, WI: ET\Lawton. ISBN 978-1430319528.

Hertzum, M., Juul, N.C., Jorgensen, N. & Norgaard, M. (2004). *Usable security and e-banking: Ease of use vis-a-vis security.* Technical Report. Retrieved 12 March 2009, from the World Wide Web: http://www.ruc.dk/~nielsj/research/papers/ebanking-tr.pdf

Herzog, A. & Shahmehri, N. (2007). User help techniques for usable security. In: Proceedings of the 2007 symposium on Computer Human Interaction for the Management of Information Technology, CHIMIT 2007: 11.
DOI: http://doi.acm.org/10.1145/1234772.1234787

Hewett, T.T., Baecker, R., Card, S., Carey, T., Gasen, J., Mantei, M., Perlman, G., Strong, G. & Verplank, W. (1996). ACM SIGCHI Curricula for Human-Computer Interaction. ACM. ISBN 0897914740 (com, uk). Chapter 2: Human-Computer Interaction, p 5.

Hewett, T.T., Baecker, R., Card, S., Carey, T., Gasen, J., Mantei, M., Perlman, G., Strong, G. & Verplank, W. (2002). ACM SIGCHI Curricula for Human-Computer Interaction. ACM. ISBN 0897914740 (com, uk). Retrieved October 5, 2010, from the World Wide Web: http://sigchi.org/cdg/.

Hodge, M.J. (2006). The Fourth Amendment and privacy issues on the "new" Internet: Facebook.com and MySpace.com. *Southern Illinois University Law Journal*, Vol. 31: 95–122.

Hofstee, E. (2008). *Constructing a good dissertation: A practical guide to finishing a masters, MBA or PhD on schedule.* South Africa: Exactica.

Hogben, G. (2007). *Security issues and recommendations for online social networks*. Position Paper. ENISA, European Network and Information Security Agency. Retrieved April 04, 2010 from the World Wide Web:
http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf.

Holtzblatt, K. & Beyer, H. (1993). Making customer-centred design work for teams. *CACM*, 36(10): 93–103.

Holtzblatt, K., Wendell, J.B. & Wood, S. (2005). *Rapid contextual design: A how-to guide to key techniques for user-centered design.* San Francisco, CA: Morgan Kaufmann.

Hughes, B., Joshi, I. & Wareham, J. (2008). Health 2.0 and Medicine 2.0: Tensions and Controversies in the Field. *Journal of Medical Internet Research*, 10(3): e23. DOI: 10.2196/jmir.1056.

Hvannberg, E.T., Law, E.L. & Larusdottir, M.K. (2007). Heuristic evaluation: Comparing ways of finding and reporting usability problems. *Interacting with Computers,* 19: 225–240.

I

Iachello, G. & Abowd, G.D. (2005). Privacy and proportionality: Adapting legal evaluation techniques to inform design in ubiquitous computing, Proceedings of the SIGCHI conference on Human factors in computing systems, April 2–7, Portland, Oregon, USA.

IAPP. (2011). *CICA releases privacy maturity model*. Retrieved September 14, 2009 from the World Wide Web: https://www.privacyassociation.org/publications/2010_08_13_cica_releases_privacy_maturity_model/

Internet World Stats. (2011). *Usage and population statistics*. Internet usage statistics: Internet the big picture. World Internet users and population stats. Retrieved August 10, 2011, from the World Wide Web: http://www.internetworldstats.com/stats.htm

ISO 13407. (1999). Human-centred design processes for interactive systems.

ISO 9241-11. (1998). Ergonomic requirements for office work with visual display terminals (VDTs) – Part 11: Guidance on usability.

ISO 9241-210. (2010). Ergonomics of human-system interaction – Part 210: Human-centred design for interactive systems.

ISO/IEC 27002. (2005). Information technology — Security techniques – Code of practice for information security management using: ISO/IEC 27002: ISO.

ISO/IEC 27799. (2008). Health informatics — Information security management in health using: ISO/IEC 27002: ISO.

J

Jessen, W. (2007). Highlight HEALTH: Web 3.0 and Predictive, Preventive and Personalized Medicine. Retrieved May 05, 2009, from the World Wide Web: www.highlighthealth.com/healthcare/Web-30-and-predictive-preventive-and-personalized-medicine/

Jick, T.D. (1979). Mixing qualitative and quantitative methods: Triangulation in action. *Administrative Science Quarterly*, 24(4): 60–611. Johnson Graduate School of Management, Cornell University. Retrieved July 16, 2008, from the World Wide Web: http://www.jstor.org/stable/2392366

Johnston, J. (2004). A framework for secure human computer interaction. MSc Dissertation, Rand Afrikaans University. Johannesburg.

Johnston, J., Eloff, J.H.P. & Labuschagne, L. (2003). Security and human computer interfaces. *Computers & Security*, 22(8): 675–684.

Jokela, T. (2001). Assessment of user-centred design process as a basis for improvement action: An experimental study in industrial settings. Dissertation, University of Oulu, Finland. ISBN 951-42-6550-5

K

Kahn, R. & Cannell, C. (1957). *The dynamics of interviewing.*, New York and Chichester: Wiley.

Kankainen, T. & Parkkinen, J. (2001). GUP: graphical presentation of user profile. CHI '01 extended abstracts on human factors in computing systems. March 31-April 05, 2001, Seattle, Washington. DOI: 10.1145/634067.634131

Karray, F., Alemzadeh, M., Saleh, J.A. & Arab, M.N. (2008). Human-computer interaction: Overview on state of the art. *International Journal on Smart Sensing and Intelligent Systems*, 1(1): 137–159.

Katsabas, D., Furnell, S.M. & Dowland, P.S. (2005). Using human computer interaction principles to promote usable security. In: *Proceedings of the Fifth International Network Conference (INC 2005)*. Samos, Greece. 5e7.

Katz, S.J. & Moyer, C.A. (September, 2004). The emerging role of online communication between patients and their providers. *Journal of General International Medicine*, 19(9): 978–983. DOI: 10.1111/j.1525-1497.2004.30432.x

Kobsa, A. (2002). Personalized hypermedia and international privacy. *Communications of the ACM*, 45(5): 64–67. DOI: 10.1145/506218.506249.

Kuhn, P. (2008, October). *Health management technology: Patient portals*. Retrieved February 26, 2009, from the World Wide Web: www.healthmgttech.com/features/2008_october/1008_thought_leaders.aspx

Kumaraguru, P. & Cranor, L. (2005). Privacy Indexes: A Survey of Westin's Studies. *ISRI Technical Report CMU-ISRI-05-138*. Retrieved October 26, 2011, from the World Wide Web: http://reports-archive.adm.cs.cmu.edu/anon/isri2005/abstracts/05-138.html

L

Law, E.L. & Hvannberg, E.T. (2004). Analysis of strategies for improving and estimating the effectiveness of heuristic evaluation, In: *Proceedings of the third Nordic conference on Human-computer interaction,* October 2004, Tampere: Finland: 241-250. Available DOI: 10.1145/1028014.1028051 (Accessed 15 November 2010).

Law, E.L. (2007). Heuristic evaluation. In Scapin, D. & Law, E. (Eds), *R3UEMs: Review, Report and Refine International Workshop,* pp 61–63, MAUSE.

Leavitt, M.O. & Shneiderman, B. (2006). Research-based Web design & usability guidelines. In: USDOHAH (Ed.), *Services.* US Government Printing Office, Washington, DC.

Lethbridge, T.C. & Laganiere, R. (2005). *Object-oriented software engineering: Practical software development using UML and Java.* Second edition. Berkshire, England: McGraw-Hill-Education.

Leventhal, L. & Barnes, J. (2007). *Usability engineering: process, products & examples.* Upper Saddle River, N.J: Prentice Hall.

Lewis, C. & Rieman, J. (1994) *Task-centered user interface design: A practical introduction*. Retrieved December 2, 2010 from the World Wide Web: http://hcibiborg/tcuid/chap-4.html

Ling, C. & Salvendy, G. (2005). Extension of heuristic evaluation method: a review and re-appraisal. International *Journal of Ergonomics and Human Factors*, 27(3): 179–197.

Lues, L. & Lategan, L. (2006). *Research ABC*. Stellenbosch: SUN.

M

Madden, M. & Zickuhr, K. (2011). *Pew Research Center: 65% of online adults use social networking sites*. Retrieved October 05, 2011, from the World Wide Web: http://pewinternet.org/Reports/2011/Social-Networking-Sites.aspx

Markus, M.L. (1983). Power, politics and MIS implementation. *Communications of the ACM*, 26: 430–444.

Maxwell, J.A. (2005). *Qualitative research design: An interactive approach.* Second edition. Applied social research methods series Vol. 41. Thousand Oaks, CA: Sage

McGrow, K., Horsman Brennan, A. & Preece, J. (2004) Development of a tool for heuristic evaluation of healthcare information systems. *Computers, Informatics, Nursing, Journal of Hospice & Palliative Nursing*.

McHugh, M.L. & Villarruel, A.M. (2003). Descriptive statistics, Part I: Level of measurement. *Journal for Specialists in Pediatric Nursing*, 8(1): 35.

Merriam, S.B. (2001). *The new update on adult learning theory.* San Francisco, CA: Jossey-Bass.

Metz, C. (2007). *PC Magazine: Web 3.0.* Retrieved May 05, 2009, from the World Wide Web: www.pcmag.com/article2/0,2817,2102852,00.asp

Miles, M.B. & Huberman, A.M. (1994). *Qualitative data analysis.* Second edition. Thousand Oaks, CA: Sage

Millen, D.R. (2000). Rapid ethnography: time deepening strategies for HCI field research. In *Proceedings of the conference on Designing interactive systems: processes, practices, methods, and techniques*: 280-286. New York City.

Molich, R. & Nielsen, J. (1990). Improving computer dialogue. *Comm, ACM*, 33(3): 338–348.

Mortimer, R. (2007). Sharpen your SEO weapons for Web 3.0's robot marketing wars. *Marketing Week* (01419285), 30(47): 17. From MasterFile Premier Database.

Morville, P. (2004). *Facets of the user experience*. Retrieved August 04, 2009, from the World Wide Web: http://semanticstudios.com/publications/semantics/000029.php

Muller, G. (2006). *The present and the future of usable security*. Retrieved 27 February 2009 from the World Wide Web: http://ec.europa.eu/information_society/istevent/2006/cf/document.cfm?doc_id=1954

Myers, M.D. (1997). Qualitative research in information systems. *MIS Quarterly* 21(2): 241–242. *MISQ Discovery*, archival version, http://www.misq.org/discovery/MISQD_isworld/. *MISQ Discovery*, updated version, last modified: January 4, 2008. Retrieved July 19, 2009, from the World Wide Web: www.qual.auckland.ac.nz

N

National Cyber Security Alliance. (2011a). *2011 NATIONAL SMALL BUSINESS STUDY*. Retrieved October 05, 2011, from the World Wide Web: http://www.staysafeonline.org/sites/default/files/resource_documents/2011%20SMB%20Study%20.pdf

National Cyber Security Alliance. (2011b). *In the Home: Protect Yourself. Social Networking*. Retrieved October 05, 2011, from the World Wide Web: http://www.staysafeonline.org/in-the-home/social-networking

Newell, A. & Card, S.K. (1986). Straightening out softening up: Response to Carroll and Campbell. *Human-Computer Interaction,* Vol. 2: 251–267.

Nielsen J. (1993). *Usability engineering*. San Diego, CA: Morgan Kaufmann.

Nielsen, J. (1994). Heuristic evaluation. In: Nielsen J. & Mack, R.L. (Eds.), *Usability inspection methods*. New York: John Wiley & Sons, pp 25–62.

Nielsen, J. (1997). *Useit.com: The use and misuse of focus groups*. Retrieved November 15, 2010, from the World Wide Web: http://www.useit.com/papers/focusgroups.html

Nielsen, J. (2005a). *Useit.com: Heuristic evaluation*. Retrieved October 10, 2010, from the World Wide Web: http://www.useit.com/papers/heuristic/

Nielsen, J. (2005b). *Useit.com: How to conduct a heuristic evaluation.* Retrieved October 10, 2010, from the World Wide Web: http://www.useit.com/papers/heuristic/heuristic_evaluation.html

Nielsen, J. (2005c). *Useit.com: Severity ratings for usability problems.* Retrieved October 10, 2010, from the World Wide Web: http://www.useit.com/papers/heuristic/severityrating.html

Nielsen, J. (2006). *Useit.com: Ten usability heuristics*. Retrieved October 5, 2010, from the World Wide Web: www.useit.com/papers/heuristic/heuristic_list.html

Nielsen-Norman Group (n.d). *Our definition of user experience*. Retrieved October 5, 2010, from the World Wide Web: http://www.nngroup.com/about/userexperience.html

NIST Special Publication 800-53. (2009). *Information security: Recommended security controls for federal information systems and organizations using*: *NIST* Special Publication 800-53.

O

Oates, B. J. (2006). *Researching information systems and computing*. London, Thousand Oaks, Calif: SAGE, p. 364.

Olivier, M. (2009). *Information technology research: A practical guide for computer science and informatics*. Third edition. Pretoria, South Africa: Van Schaik.

P

Paddison, C. & Englefield, P. (2004). Applying heuristics to accessibility inspections. *Interacting with Computers*, 16(2): 507–521.

Palo Alto Networks. (2010). *Network World: Top 10 social networking threats*. Retrieved October 08, 2011, from the World Wide Web: http://www.networkworld.com/news/2010/071210-social-network-threats.html?page=1

Paluch, K. (2006). *What is user experience design*? Retrieved October 10, 2010, from the World Wide Web: http://www.montparnas.com/articles/what-is-user-experience-design/comment-page-5/

Patrick, A.S. & Kenny, S. (2003). From privacy legislation to interface design: Implementing information privacy in human-computer interaction. Proceedings of the Privacy Enhancing Technologies Workshop (PET2003), Dresden, Germany, 26-28 March, 2003.

Patton, M. Q. (1990). *Qualitative evaluation and research methods*. Second edition. Newbury Park, CA: Sage.

Pettersson, J.S. & Fischer-Hübner, S. (2004). E*valuation of early prototypes, PRIME deliverable D6.1.b.* Retrieved 10 February 2011 from the World Wide Web: https://www.prime-project.eu/prime_products/reports/eval/pub_del_D06.1.b_ec_wp06.1_V4_final.pdf.

Pettersson, J.S., Fischer-Hübner, S., Danielsson, N., Nilsson, J., Bergmann, M., Clauss, S., Kriegelstein, T. & Krasemann, H. (2005). Making PRIME usable, Proceedings of the 2005 symposium on usable privacy and security, July 6–8, Pittsburgh, Pennsylvania, pp 53–64. DOI: 10.1145/1073001.1073007.

Pierotti, D. (1995). Heuristic evaluation: A system checklist, In Xerox Corporation, *Usability analysis and design*,. Retrieved October 5, 2010, from the World Wide Web: http://www.stcsig.org/usability/topics/articles/hechecklist.html

Preibusch, S., Hoser, B., Gürses, S. & Berendt, B. (2007, June). Ubiquitous social networks: Opportunities and challenges for privacy-aware user modelling. Proceedings of Workshop on Data Mining for User Modeling. Corfu, Greece. Retrieved August 4, 2009 from the World Wide Web: http://vasarely.wiwi.hu-berlin.de/DM.UM07/Proceedings/05-Preibusch.pdf

Purdy, R. (2008). *The power and the perils of using social networking tools in the NHS: A masterclass for the NHS Faculty of Health Informatics.* Retrieved 7 April 2009 from the World Wide Web: www.library.nhs.uk/SpecialistLibrarySearch/Download.aspx?resID=289920

R

Renaud, K. & De Angeli, A. (2009). Visual passwords: cure-all or snake-oil? *Communications of the ACM,* vol. 52 (12): 135-140.

Robson, C. (2002). *Real world research*. Second edition. Oxford: Blackwell.

Roessler, T. & Saldhana, A. (2009). *Web security context: User interface guidelines, W3C working draft* (work in progress). Retrieved 10 October 2009 from the World Wide Web: http://www.w3.org/TR/wsc-ui/

Rogers, Y., Sharp, H. & Preece, J. (2008). *Interaction design: Beyond human-computer interaction.* Chichester, Hoboken, NJ: John Wiley.

Rosenbaum, S., Rohn, J.A. & Humburg, J. (2000). A toolkit for strategic usability: results from workshops, panels, and surveys. In: *CHI '00: Proceedings of the SIGCHI conference on human factors in computing systems, 2000*. New York, NY: USA. ACM: 337–344.

Roto, V. (2007). User experience from a product creation perspective: Towards a UX manifesto workshop, in conjunction with HCI 2007, Lancaster, UK, pp 31–34.

Rozinov, K. (2004). *Are usability and security two opposite directions in computer systems*? White paper in Department of Computer and Information Science, Polytechnic University.

Rubin, J. & Chisnell, D. (2008). Handbook of usability testing: How to plan, design, and conduct effective tests. Second edition, New York: John Wiley.

S

Saffer, D. (2009*). Designing for interaction*. Second Edition, Berkeley, CA: New Riders.

Sasse, M. & Flechais, I. (2005). Usable Security Why do we need it? How do we get it? In: Cranor, L.F. & Garfinkel, S. (Eds.). *Security and Usability: Designing Secure Systems That People Can Use*. Sebastopol, CA: O' Reilly Media Inc., p.13-30.

Saunders, S., Lewis, P. & Thornhill, A. (2000). *Research methods for business students*. Second Edition. London: Prentice Hall.

Saunders, S., Lewis, P. & Thornhill, A. (2007). *Research methods for business students*. Fourth edition. London: Prentice Hall.

Shneiderman, B. (1995). *The front desk*. BBC Video.

Sim, G., Read, J.C. & Cockton, G. (2009). Evidence based design of heuristics for computer assisted assessment. In: *Proceedings of the 12th IFIP TC 13 International Conference*. Uppsala: Sweden.

Somervell, J. & McCrickard, D.S. (2005). Better discount evaluation: illustrating how critical parameters support heuristic creation. *Interacting with Computers,* vol. 17: 592–612.

Soy, S.K. (1997). *The case study as a research method*. Retrieved December 19, 2009, from the World Wide Web: http://fiat.gslis.utexas.edu/~ssoy/usesusers/l391d1b.htm

Straub, K. (2003). Pitting usability testing against heuristic review. *UI Design Update Newsletter*. Retrieved December 18, 2009, from the World Wide Web: http://www.humanfactors.com/downloads/sep03.asp.

Straub, T. & Baier, H. (2004). A framework for evaluating the usability and the utility of PKI-enabled applications. In: *EuroPKI 2004: Proceedings of the 1st Europeann PKI Workshop: Research and Applications.* Springer, Samos Island, Greece, pp. 112-125.

Strauss, A.L. (1987). *Qualitative analysis for social scientists*. Cambridge, UK: Cambridge University Press.

T

Te'eni, D. (2006). Designs that fit: An overview of fit conceptualizations in HCI. In: . Zhang, P. & Galletta, D. (Eds), *Human-computer interaction and management information systems: Foundations.* Armonk, NY: ME Sharpe.

Thurmond, V. (2001). The point of triangulation. *Journal of Nursing Scholarship*, 33(3): 254–256. Retrieved March 10, 2011, from the World Wide Web: http://www.ruralhealth.utas.edu.au/gr/resources/docs/the-point-of-triangulation.pdf.

Trauth, E. M. & Jessup, L.M. (2000). Understanding computer-mediated discussions: Positivist and interpretive analyses of group support system use. *MIS Quarterly,* 24(1).

Trochim, W. (2006a). *Research methods knowledge base: Descriptive statistics*. Retrieved July 05, 2011, from the World Wide Web: www.socialresearchmethods.net/kb/statdesc.php

Trochim, W. (2006b). *Research methods knowledge base: Ethics in research*. Retrieved March 19, 2011, from the World Wide Web: http://www.socialresearchmethods.net/kb/ethics.php

Trochim, W. & Donelly, J.P. (2006). *The research methods knowledge base.* Third edition. Cincinnati, OH: Atomic Dog.

U

UXBASIS (n.d.). *About*. Retrieved July 04, 2011 from the World Wide Web: http://uxbasis.hellogroup.com/about/

V

Van der Merwe, A.J., Kotze, P. & Cronje, J. (2005). The functionality of a requirements elicitation procedure developed within the Higher Education domain. *Alternation*, 12(1): 489–514.

Van Greunen, D. (2009). A framework for the user interface design of business process management tools. PhD Thesis, University of South Africa, Pretoria.

Vredenburg, K., Mao, J., Smith, P.W. & Carey, T. (2002). A survey of user-centered design practice. In*: Conference on Human Factors in Computing Systems; SIGCHI Conference on Human Factors in Computing Systems: Changing Our World Changing Ourselves,* pp 471–478.

W

Web Credibility Project. (2007). *Stanford Web credibility research*. Retrieved August 04, 2009 from the World Wide Web: http://credibility.stanford.edu/

Whitten, A. & Tygar, J.D. (2005). Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In: Cranor, L. & Garfinkel, S. (Eds.), *Security and usability: Designing secure systems that people can use.* Sebastopol, CA: O'Reilly, pp 669–692.

Woolrych, A. & Cockton, G. (2001). Why and when five test users aren't enough. In: Vanderdonckt, J., Blandford, A. & Derycke, A. (Eds.), Proceedings of IHM-HCI 2001. Toulouse, France: *Cépadèus,* Vol. 2: 105–108.

Wright, P., Blythe, M. & McCarthy, J. (2006). User experience and the idea of design in HCI. Interactive Systems: 12th International Workshop, DSVIS 2005, Newcastle upon Tyne, UK, July 13-15, 2005. *Revised Papers Lecture Notes in Computer Science,* Vol. 3941: 1–14

Y

Yee, K. (2002). User interaction design for secure systems. In: *Proceedings of the 4th International Conference on Information and Communications Security*, 2002 (ICICS' 02), Springer-Verlag, London, UK, pp 278–290.

Yeratziotis, A., Pottas, D. & van Greunen, D. (2011a). A Three-Phase Process to Develop Heuristics, *13th ZA-WWW conference*, 14–16 September 2011, Johannesburg.

Yeratziotis, A., Pottas, D. & van Greunen, D. (2011b). Recommendations for Usable Security in Online Health Social Networks. *In Proceedings of the joint conference of the 2011 6th International Conference on Pervasive Computing and Application (ICPCA) and the 2011 3rd International Symposium of Web Society (SWS)*, 26-28 October 2011, Port Elizabeth, South Africa.

Yeratziotis, A., Pottas, D. & van Greunen, D. (2012). A usable security heuristic evaluation for the online health social networking paradigm. *International Journal of Human-Computer Interaction*, vol. 29(3).

Yeratziotis, A., Sannemann, C., Viitanen, J. & Nieminen, M. (2011). Analysis of Emergent Use for Wellbeing Service Innovation. *Design, User Experience, and Usability, Pt I, HCII 2011*, LNCS 6769, pp. 332–341, 2011. Springer-Verlag Berlin Heidelberg 2011.

Yin, R.K. (2008). *Case study research: Design and methods.* Fourth edition. London: Sage.

Z

Zickmund, S.L, Hess, R., Bryce, C.L, McTigue, K., Olshansky, E., Fitzgerald, K. & Fischer, G.S. (2007). Interest in the use of computerized patient portals: Role of the provider–patient relationship. *Journal of General Internet Medicine*, Suppl 1: 20–26. DOI: 10.1007/s11606-007-0273-6.

Zimmerman, J., Forlizzi, J. & Evenson, S. (2007). Research through design as a method for interaction design research in HCI. In *CHI '07: Proceedings of the SIGCHI conference on Human factors in computing systems*, New York, NY, USA. ACM, pp 493–502.

Zurko, M.E. & Johar, K. (2008). *Standards, usable security, and accessibility: Can we constrain the problem any further?* Retrieved 10 February 2009 from the World Wide Web: http://cups.cs.cmu.edu/soups/2008/SOAPS/zurko.pdf

INDEX OF APPENDICES ON CD-ROM

Section	Description	Total Appendices
A	Contributions	2
B	Results from Participants	44 (7 per participant + 2 examples of the consent forms that participants signed on MedHelp and Google Health)
C	Results from Experts	4 (1 per expert)
D	Requirements for OHSNs	2
E	Publications	7

Title	Description
Appendix A.1	USec HE
Appendix A.2	Validation Tool Template
Appendix B.1	Biographical Information
Appendix B.2	Scenarios and Tasks (MedHelp)
Appendix B.3	Scenarios and Tasks (Google Health)
Appendix B.4	USec HE (MedHelp)
Appendix B.5	USec HE (Google Health)
Appendix B.6	Comparison MedHelp & Google Health
Appendix B.7	User Satisfaction Questionnaire
Appendix B.8	Biographical Information
Appendix B.9	Scenarios and Tasks (MedHelp)
Appendix B.10	Scenarios and Tasks (Google Health)
Appendix B.11	USec HE (MedHelp)
Appendix B.12	USec HE (Google Health)
Appendix B.13	Comparison MedHelp & Google Health
Appendix B.14	User Satisfaction Questionnaire
Appendix B.15	Biographical Information
Appendix B.16	Scenarios and Tasks (MedHelp)
Appendix B.17	Scenarios and Tasks (Google Health)
Appendix B.18	USec HE (MedHelp)
Appendix B.19	USec HE (Google Health)
Appendix B.20	Comparison MedHelp & Google Health
Appendix B.21	User Satisfaction Questionnaire
Appendix B.22	Biographical Information
Appendix B.23	Scenarios and Tasks (MedHelp)
Appendix B.24	Scenarios and Tasks (Google Health)
Appendix B.25	USec HE (MedHelp)
Appendix B.26	USec HE (Google Health)
Appendix B.27	Comparison MedHelp & Google Health
Appendix B.28	User Satisfaction Questionnaire
Appendix B.29	Biographical Information
Appendix B.30	Scenarios and Tasks (MedHelp)
Appendix B.31	Scenarios and Tasks (Google Health)
Appendix B.32	USec HE (MedHelp)
Appendix B.33	USec HE (Google Health)
Appendix B.34	Comparison MedHelp & Google Health