APPENDIX A: FRAMEWORK EVALUATION TOOL

SECTION A: Introduction

My name is [REMOVED]. I invite you to participate in this framework evaluation process. The purpose of this evaluation tool is to validate the proposed socio-technical information security (STInfoSec) framework for the design of secure and usable online information security applications.

The [REMOVED] study entitled "A Socio-Technical Framework for Secure and Usable Online Information Security Systems". The framework is specifically designed for online banking service as a case study, but is intended to be applicable to other general online information security applications, with appropriate adaptations tailored to those applications. The principles provided here for evaluation were first selected from previous studies in literature, then based on survey and interview findings from online banking users and banking personnel, respectively, the list has been refined in the context of online banking service. Checklist items for each principle were developed into this preliminary framework.

As an evaluator, you are requested to rate the importance of each of the proposed design principles and their respective checklist items with regard to their relevance in addressing security- and usability-related problems of the service. Specifically, these principles are envisaged to assist the design and, ultimately, improve the service. Your participation in this study is highly appreciated.

Please kindly complete and submit the evaluation survey to the researcher as soon as possible. The evaluation tool will take at most approximately 60 minutes to complete.

SECTION B: Consent form

Please note that by submitting this form, you agree that you have not been put under any pressure to participate in this evaluation exercise and are willingly participating in it. Also, please note that participation is voluntary and that you may withdraw at any time without negative consequences. Please understand that your answers to these questions will be used for academic purposes only; likewise, the findings of the evaluation will be used for research purposes only and may be published in academic publications. Your privacy will be protected by not printing any names, positions, or institutions in any such publication. The data will be stored in a password-protected computer and locked file cabinet at Unisa for a period of five years, after which it will be incinerated.

Please tick the checkbox to voluntarily provide consent to participate in the study.

I accept ☐

SECTION C: Instructions

All questions marked with an asterisk (*) need to be answered. The information requested in Section D is for verification purposes only and responses will only be identified through a pseudo name/number, with no reference to any individual whatsoever.

Section E consists of the checklist items that system designers need to address. There are 12 usable security principles specifically tailored to online banking service. Each principle has a varying number of checklist items, ranging from five to nine, that help in understanding and applying the principle during the design of the user interface. We request your input in rating the importance of each of the checklist items to determine the usefulness of the principle as a whole. Each checklist item is rated based on a scale with the following four options: very important, important, moderately important, and not important. Evaluators are requested to provide additional information that they think might improve the framework at both a checklist and a principle level.

SECTION D: Biographical information

Please note that the information requested here is for verification purposes only; your responses will only be identified through a pseudo name/number, with no reference to your name whatsoever.

Full name				
Gender	Male		Female	
Age				
Qualification				
Occupation				
Job title				
Job specialisation				
Years in position				
IT/IS security experience				
Usability/UX experience				
Usable security experience				
Other experience (please specify)				

SECTION E: Checklist items

Your assessment is based on the importance of the 12 principles and their respective checklist items in addressing security and usability aspects of system development. Additional comments are welcome at both a checklist item and a principle level.

Please indicate your choice by selecting one of the provided options as follows: 1 = Not important, 2 = Moderately important, 3 = Important, and 4 = Very important.

1	**Visibility: the system should visibly keep users informed about their security status**
1.1	Does the system show the user the progress status during a visible delay in response time?
1.2	Does the system visibly show the current selection/data input field?
1.3	Does the system clearly highlight the problem field with regard to error messages?
1.4	Is there some form of feedback for every security-related action?
1.5	Does the system visibly show the location of security-related options?
1.6	Is help information for assisting the user visible and easily accessible?
	Additional comments (optional)
2	**Learnability: the system should ensure that security actions are easy to learn and remember**
2.1	Does the system provide easy-to-learn training material?
2.2	Is there a quick-start guide to assist the user?
2.3	Are security and non-security operations easy to learn and use?
2.4	Have security items been grouped into logical zones, and have headings been used to distinguish between the zones?
2.5	Does the system present security and non-security information in a standardised format?
2.6	Are security options selected by default?
2.7	Does the user interface make it obvious which security items are currently selected?
2.8	Does the system protect users against making severe errors?
	Additional comments (optional)
3	**Errors: the system should provide users with detailed security error messages that they can understand and act on**
3.1	Are system error messages grammatically correct and accurate in stating the problem, with enough information for

	corrective measures/actions?
3.2	Do security-related error messages inform the user of the severity of the error?
3.3	Are menu items arranged logically to prevent users from making serious errors?
3.4	Does the system warn users if they are about to make a potentially serious error?
3.5	Does the system allow users to recover from errors quickly and easily?
3.6	Do the error messages of the system not interfere with the users' work, whenever possible?
3.7	Does the system clearly ask for users' confirmation of serious and possibly irrevocable actions?
	Additional comments (optional)
4	**Availability: system services must be available all the time, with minimum down time, and have minimum interruptions**
4.1	Is the system always available, with minimum and non-interruptive down time?
4.2	Does the system make sure that all system functionalities are available at all times?
4.3	Is scheduled down time communicated in advance and scheduled during off-peak times?
4.4	Does the system limit the frequency of changes to the user interface?
4.5	Do updates to the system user interface not result in users having to learn the system all over again?
	Additional comments (optional)
5	**Satisfaction: the system should ensure that users have a good experience when using the system and its security features**
5.1	Is the actual process of using the system fun and enjoyable?
5.2	Are the most frequently used function keys in the most accessible positions?
5.3	Do security-related prompts imply that the user is in control?
5.4	Is each individual security setting a member of a family of security options?
5.5	Do the security mechanisms of the system provide a sense of protection to the user?
5.6	Has colour been used specifically to draw attention, communicate organisation, indicate status changes, and establish relationships for security- and non-security-related actions?
5.7	Can users personalise their own system, session, file, and screen defaults, such as the landing page?
5.8	Does the system fulfil its claimed capabilities?
5.9	Does the system complete unambiguous partial input on a data entry field?
	Additional comments (optional)
6	**Revocability: the system should allow users to revoke any of their security actions**
6.1	Do security options in menus make it obvious whether deselection is possible?
6.2	Can users easily reverse their security and non-security actions?
6.3	When prompts imply a necessary security action, are the words in the message consistent with that action?
6.4	Has the system been designed so that keys with similar names do not perform opposite (and potentially dangerous) security actions?
6.5	Can users cancel operations in progress?
6.6	Are there 'undo' and 'redo' functions at the level of a single security action or for a complete group of security actions?
6.7	Does the system provide confirmation for actions that have drastic, possibly destructive consequences?
6.8	Does the system have a clearly marked exit?
	Additional comments (optional)

7	**Expressiveness: the system should guide users on security in a manner that still gives them freedom of expression**
7.1	Are users initiators of security actions rather than respondents?
7.2	Does the system correctly anticipate, and prompt for, the user's probable next security-related activity?
7.3	By looking, can the user tell the security state of the system and the alternatives for security-related actions, if needed?
7.4	Does the system clearly state its security capabilities?
7.5	Does the system clearly state the users' responsibilities in terms of security actions?
	Additional comments (optional)
8	**User language: the system should use plain language that users can understand with regard to security**
8.1	Does the system allow the user to choose a preferred language?
8.2	Are security actions and objects named consistently across all prompts in the design?
8.3	Is security information accurate, complete, and understandable?
8.4	Are security questions stated in clear and simple language, where used?
8.5	If language selection is possible, is the translation accurate, without errors?
	Additional comments (optional)
9	**User suitability: the system should provide options for users with diverse levels of skill and experience in security**
9.1	Is security information accurate, complete, and understandable to all types of system users (experienced and novice)?
9.2	Can users define and group their own synonyms for commands for easier access?
9.3	Can users navigate forwards and backwards within operations?
9.4	Does the system avoid the use of security and privacy jargon?
9.5	If the system supports both novice and expert users, are multiple levels of error message detail available?
	Additional comments (optional)
10	**Help and documentation: the system should make security help apparent and easy to find for users**
10.1	Is the help function visible, for example, a key labelled HELP or a special menu?
10.2	Is it easy to access, and return from, the help function, allowing users to resume their work from where they left off after accessing help?
10.3	Does the help function cover security- and non-security-related information?
10.4	Does the system provide an up-to-date security centre, with security training and awareness information?
10.5	Does the system provide a 24-hour help desk for critical security incidents?
10.6	Does the system provide complete and accurate help and a FAQs section?
10.7	Is the help and FAQs material searchable and grouped in logical categories?
10.8	Does the system provide detailed training and education material on how to complete basic tasks?
10.9	Does the system provide a search function for locating system functions?
	Additional comments (optional)
11	**Security: the system should provide trusted communication channels between the user and the data servers**
11.1	Do critical transactions require out-of-band authentication such as an OTP/SMS?
11.2	Does the system initiate a session lock after a period of inactivity or on user request?

11.3	Does the system employ encryption techniques to prevent unauthorised disclosure of, and access to, information in storage and transmission?
11.4	Does the system enforce a limit on consecutive invalid access attempts by a user during a period of time?
11.5	Does the system implement an appropriate time-out logoff period?
11.6	Does the system encrypt passwords in storage and in transmission?
11.7	Does the system enforce password restrictions, such as complexity, length, expiry period, reuse, etc.?
11.8	Are system password requirements complex enough to avoid simple password-cracking attacks?
	Additional comments (optional)
12	**Privacy: the system should protect user information against unauthorised access by third parties**
12.1	Does the system ask for consent before collecting personal information?
12.2	Are the statements asking for user consent written in clear and simple language that the user understands?
12.3	Does the system clearly state what personal information is collected and for what purposes it will be used?
12.4	Does the system require users to confirm statements indicating that they understand the conditions of access?
12.5	Does the system ask for permission before distributing personal information to third parties?
12.6	Do the personal information collection and storage mechanisms comply with the data protection regulations of the country?
12.7	Can protected or confidential areas be accessed with certain passwords?
	Additional comments (optional)

Thank you very much for your participation

Thank you once again for your participation and please feel free to contact me or the study promoters with any questions on the contact details below:

[NAMES REMOVED]