Managing the development of secure electronic banking

Tom Nilsen

Master's Thesis
Master of Science in Information Security
30 ECTS
Department of Computer Science and Media Technology
Gjøvik University College, 2006

Institutt for
informatikk og medieteknikk
Høgskolen i Gjøvik
Postboks 191
2802 Gjøvik

Department of Computer Science
and Media Technology
Gjøvik University College
Box 191
N-2802 Gjøvik
Norway

Preface

To start with a higher degree of education in a mature age is fascinating. One get to learn how little one knows and how different perspectives and abstraction levels can change a view.

Three years of part-time study besides work has certainly created a tight schedule and clear priorities to get through, which has taken its toll from one's surroundings.

But the reward - a broad and modern overview of the field of information security - has made it worth while.

This Master thesis concludes it all by challenging ones ability to express clear problems, adequate methods, up to date knowledge and then build ones own – small - contribution on top.

One feels privileged to have had this peek into the scientific world and would like to thank those who have made it possible:

- My wife who is – still - married to me and has provided invaluable support during the 3 years
- My Bank and my manager who have arranged a realistic situation for me as apart time student
- My Supervisor for giving me a perfect balance between detailed guidance and personal thrust
- My fellow students, friends, colleagues and others who has given me valuable comments

Abstract

This MSc project is an assignment from a bank.

Security has always been important to banks. With Electronic banking, it has become even more important, as Internet may supersede the retail outlets as a distribution channel for financial products and services.

The further growth of electronic banking is dependent on the level of trust from customers, the society and media, and this trust may be reduced by security incidents and bad publicity.

The bank has regularly been improving the security process in developing new IT systems. This area got increased focus with the introduction of Internet banking and e-commerce.

The vision for this security process is a proper balance between:

- Business needs – including Confidentiality, Integrity and Availability
- Security and risk management requirements
- Ease of use
- Ease of (security) administration

The bank has good reasons to believe that the process and Security analysis *early in the project phase* constitutes a right approach. But, *the Bank does not know* what contribution the security process and analysis have had on that result.

The Bank therefore needs to develop a security metric to measure the security status of the system when it is delivered from the development process.

The primary function of the metric is to:

- Document the security status for risk management and compliance purposes
- Measure the effect of the security process and indicate areas of improvement

The main goal of the security process is to manage operational risk associated with IT systems. Analyses of the areas of non-compliance, the associated risk and the root cause will be important parts of the Bank's risk management.

We have tested and improved a prototype security metric that lays a good foundation for a final Norwegian metric according to the assignment from the Bank. In section *Further work* we have described the necessary steps to achieve this final metric. We have also acquired a detailed insight in the Bank's related security documents, which can be used to improve them and the related security process at a later stage.

Prof. Slobodan Petrovic at Gjøvik University College has been Supervisor for this thesis.

Sammendrag

Dette MSc prosjektet er en oppgave fra en bank.

Sikkerhet har alltid vært viktig for banker. Med Nettbank har det blitt ennå viktigere etter som Internet kan overstige filial og kontornettets viktighet som distribusjonskanal for finansielle produkter og tjenester.

Den videre veksten for Nettebank er avhengig av tillit fra kunder, samfunnet og media, og denne tilliten kan bli redusert ved sikkerhetshendelser og negativ publisitet.

Banken har jevnlig forbedret sikkerhetsprosessen for utvikling av nye IT-systemer. Dette området fikk økt fokus ved introduksjon av Nettbank og e-handel.

Visjonen for sikkerhetsprosessen er en god balanse mellom:

- Forretningsbehov – inkludert Konfidensialitet, Integritet og Tilgjengelighet
- Sikkerhets og risikostyringskrav
- Enkel å bruke
- Enkel å (sikkerhets) administrere

Banken har god grunn til å tro at prosessen og sikkerhetsanalysen tidlig i prosjektfasen er en fornuftig tilnærming. Men Banken vet ikke hvilket bidrag sikkerhetsprosessen og analysen har hatt på resultatet.

Banken trenger derfor å utvikle en sikkerhetsmetrikk for å måle sikkerhets status på et IT system når dette blir levert fra utviklingsprosessen.

Hovedformålet for metrikken er å:

- Dokumentere sikkerhets status til bruk for risikostyring og kontroll
- Måle effekten av sikkerhetsprosessen og indikere forbedringsområder

Hovedformålet med sikkerhetsprosessen er å styre operasjonell risiko i forbindelse med IT-systemer. Analyse av områder som har avvik fra sikkerhetskrav, den tilhørende risiko og den bakenforliggende årsak til avviket vil være viktige komponenter i Bankens risikostyring.

Vi har utviklet, testet og forbedret en prototyp på metrikken som et godt grunnlag for en endelig norsk utgave, slik dette er avtalt i oppgaven fra Banken. I seksjonen *Videre arbeid* (Further work) har vi beskrevet de nødvendige steg for å gjøre metrikken endelig ferdig. Vi har også opparbeidet en detaljert innsikt i Bankens sikkerhetsrelaterte dokumenter, som kan brukes til forbedring av dem senere.

Prof. Slobodan Petrovic, Gjøvik University College har vært veileder for dette prosjektet.

Keywords and Abbreviations

Keywords:

Information Security, Information Assurance, Security Management, Security Metrics, Security Measurement, Security Status, System development, Compliance.

Abbreviations used in this report:

ABBREVIATION	MEANING
ISF	Information Security Forum [2]
SOGP	Standard Of Good Practice – see ISF
CB and CBA	Critical Business and Critical Business Application – see SOGP
CIA	Confidentiality, Integrity and Availability
NIST	National Institute of Standards and Technology, see [4]
BSR	The Bank’s Baseline Security Requirements
SSO	Single Sign-On
POL	Norwegian Privacy act [36]
FPOL	Regulations for POL [37]

Table of contents

Managing the development of secure electronic banking 1
Preface 3
Abstract 4
Sammendrag 5
Keywords and Abbreviations 6
Table of contents 8
List of figures 10
1 Introduction 13
1.1 Problem description 13
1.2 Justification, motivation and benefits 15
1.3 Research question 16
2 Review of previous work 19
2.1 Theory on security metrics 19
2.2 Measuring Security in practice 20
3 Summary of claimed contributions 23
4 Choice of methods 25
4.1 The Author's role 25
4.2 To define a framework for the security metric 25
4.2.1 ISF's metrics 26
4.2.2 Reliability 26
4.2.3 Summary of methods 27
4.3 To define the topics to be measured in the Security status 27
4.4 To test, improve and use the metric 28
4.5 General MSc thesis 29
5 Defining a framework for the metric 31
5.1 A method for security metric design 32
5.1.1 The three-step method 33
5.1.2 Who we measure for: the stakeholders 34
5.1.3 “Clear line of sight” and accountability 39
5.1.4 The effect of measuring - "You become what you measure" 40
5.1.5 Other issues from the lecture [28] 40
5.2 The principles given in NIST Special Publications 800-55 41
5.2.1 Security program maturity 41
5.2.2 NIST 800-55 Metric detail form 43
5.3 The principles in the ISF metrics 45
5.3.1 Information Security Forum (ISF) 45
5.3.2 The Standard Of Good Practice - SOGP 46
5.3.3 The survey 49
5.3.4 Security Health check 51
5.3.5 Factors that reduces security incidents 53
5.4 A summary of the chosen framework 57
6 Defining the content of the metric 59
6.1 Background on the Bank’s security approach 59
6.1.1 Challenges related to the Bank’s documents and analyses performed... 62

6.2 The Security analysis 62
6.2.1 The control selection by Application type 63
6.3 The content analysis of the Security analysis 66
6.4 The content analysis of the Bank’s security requirements (BSR) 68
6.5 External validity: ISF's Standard of good practice - SOGP.............................. 69
6.6 BSR and SOGP CB cross referenced to the Security analysis............................ 71
6.7 Work sheet for designing the security metric 73
6.8 Considerations for the MSc thesis...76
7 Testing and improving the metric..79
7.1 Testing and developing the metric on the first system 79
7.1.1 Choosing a candidate 79
7.1.2 The first test candidate 79
7.2 Analysing the result and improving the metric 87
7.3 To measure and analyse the next candidate 87
7.3.1 The second test candidate... 87
8 Analysing the thesis's work and findings 95
8.1 Evaluating the metric 95
8.2 The secondary purpose of the metric...97
8.3 The Authors role 98
8.4 How to generalize the metric 100
8.5 Further work.. 101
8.6 ISF META standard and metrics...103
8.7 Findings – not related to the research question 104
8.8 Ethical and legal considerations 104
9 Conclusion 105
10 References 107

List of figures

Figure 1 Security in development projects 14

Figure 2 The relations that lead to secure systems 15

Figure 3 Measuring within project scope 16

Figure 4 From “A framework for Security Metrics” 20

Figure 5 Security in development projects 31

Figure 6 Three-step method [5] 32

Figure 7 The need to comply (ISF) 36

Figure 8 ISF: Sarbanes-Oxley - Implications for Information Security 37

Figure 9 Measuring within project scope 39

Figure 10 NIST: Security program maturity and types of measurement 41

Figure 11 ISF: ASPECTS in SOGP 46

Figure 12 SOGP Sample 48

Figure 13 Sample form in ISF Survey 49

Figure 14 ISF: Calculating security ratings 51

Figure 15 Sample from ISF SOGP CB 52

Figure 16 Sample from ISF Health Check 53

Figure 17 ISF: FIRM spider graph 54

Figure 18 Risk factors from Test 1 55

Figure 19 ISF: Three stage model of evolution 61

Figure 20 Application types 64

Figure 21 Content analysis of the Security analysis 68

Figure 22 ISF: ASPECTS in SOGP 69

Figure 23 BSR Cross reference 73

Figure 24 Security in system development 74

Figure 25 Security Metric work sheet 76

Figure 26 Risk factors from test 1 80

Figure 27 ISF: Sample from Health Check 86

Figure 28 Risk profile second candidate 88

Figure 29 NIST 800-55 sample Audit trail 91

Figure 30 A process for measuring [34] 101

Figure 31 New generation of tools 104

1 Introduction

Security has always been important to banks. With Electronic banking, it has become even more important, as Internet banking may supersede the retail outlets as a distribution channel for financial products and services.

The further growth of electronic banking is dependent on the level of trust from customers, the society and media, and this trust may be reduced by security incidents and bad publicity.

Generally the security focus has been directed towards the business critical systems in production, but this approach has a challenge. The budgets for system maintenance and IT operation are generally too small to have room for substantial security improvements and redesigns. If the system is not secure by delivery, it may never be - fundamentally - corrected.

Security weaknesses can be analyzed and focused on but lack of funding may limit the security actions to tactical ones.

New projects represent "fresh funding" which can be used to get security right from the start.

Security can be planned more ideally to achieve an advantage of scale in the security field by reusing secure components with user-friendly solutions and achieve lower operational and administrative cost.

The bank has regularly been improving the security process in developing new IT systems. This area got increased focus with the introduction of Internet banking and e-commerce.

The development process requires projects to go through a formal Security analysis. The analysis tool is developed by the Bank and more than 400 Security analyses have been performed and archived since 1997.

The Bank has a security framework with baseline security requirements that is similar to ISO 17799 [1]. The Security analysis is designed to support the implementation of these baseline security requirements. It starts with a simple risk analysis that indicates the business need for Confidentiality, Integrity and Availability (CIA) and continues with approx 60 security recommendations, objectives and related questions.

The analysis gives structure to the dialogue between the consultant from IT Security Department and the project manager. The goal is to convey a business perspective of risk to the IT Security consultant and convey security knowledge and motivation to the project.

The result from this security process should be a proper balance between:

- Business needs – included CIA
- Security and risk management requirements
- Ease of use
- Ease of (security) administration

1.1 Problem description

As described, the Bank has a defined security process and a Security analysis to support this process. The Bank believes that this Security analyses will set the project in a right direction, and clarify the main security considerations early in the project.

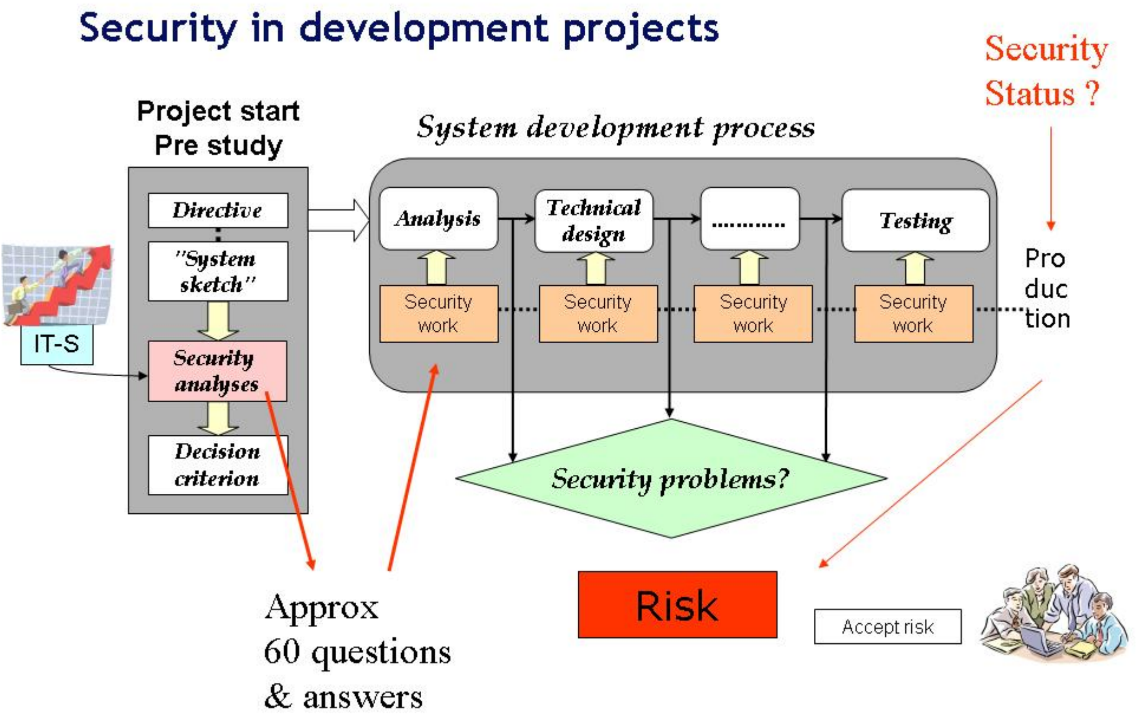


Figure 1 Security in development projects

The problem is that we do not *know* what security related results this process and analysis tool is contributing with. We have no proof or measurement that a "good" Security analysis will result in a system that is secure by delivery.

System development theory supports that security has to be planned from the start to achieve secure systems, and the Security analysis is therefore required in the planning phase of the project.

The trade off is that in the beginning, one has to focus on the overview of security. Topics like business requirements for security, design principles for security and promoting standard security solutions can give this overview.

The Baseline Security Requirements document (BSR) contains approx 200 requirements, and the Security analysis contains approx 60 questions. By answering “We will implement Single Sign-On (SSO) as recommended”, the project may partly cover 20 requirements that the SSO solution is verified to solve.

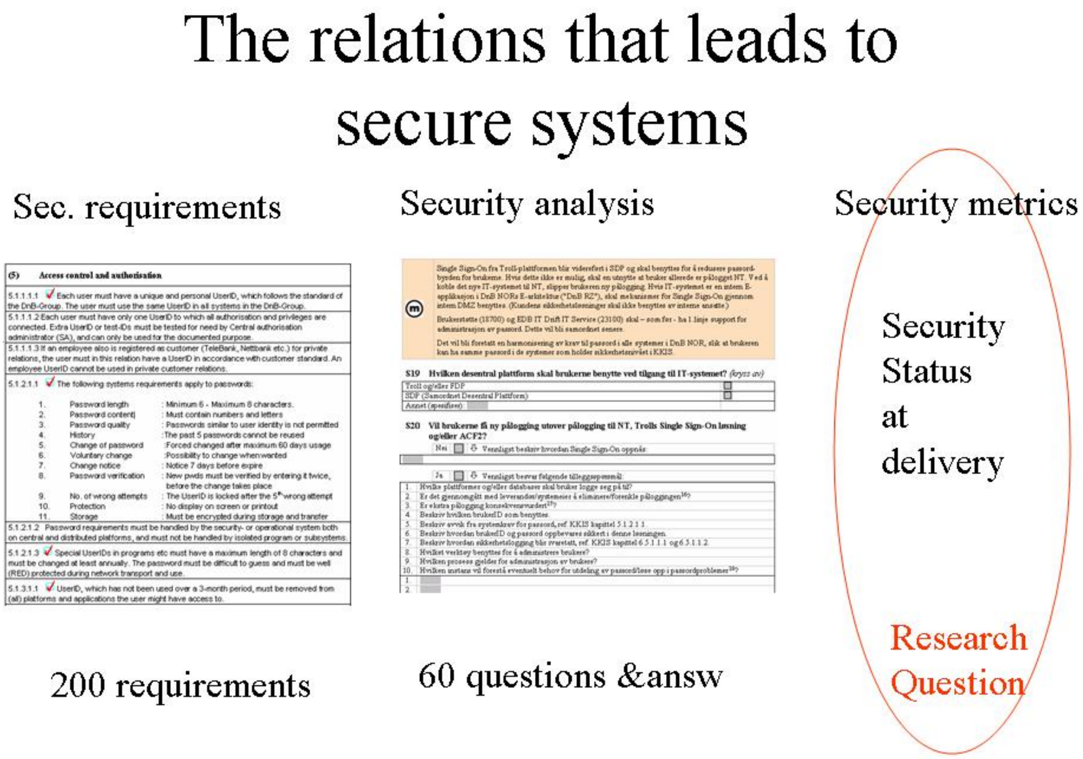
To focus on operational details of security at this stage has little meaning as the project manager - mentally - is in the start-up phase and has a holistic view.

Ideally there should be several iterations in the security process to define the refined level of security details as the project progresses. There is no guaranty that this is done properly in the project or that the project has the skills to take care of all security details.

The Security department has limited resources and cannot assist all projects in all phases of the security iterations. The choice has been to assist the project in analysing security early in the project at the cost of less attention from the Security department during the rest of the project.

The bank has good reasons to believe that the process and analysis *early in the project phase* constitutes a right approach. But, *the Bank does not know* what contribution the security process and analysis have had on that result.

The Bank therefore needs to develop a security metric to measure the security status of the system when it is delivered from the development process.



The relations that leads to secure systems

Sec. requirements

(5) **Access control and authorisation**

5.1.1.1.1 ✓ Each user must have a unique and personal UserID, which follows the standard of the DnB-Group. The user must use the same UserID in all systems in the DnB-Group.

5.1.1.1.2 Each user must have only one UserID to which all authorisation and privileges are connected. Extra UserID or test-IDs must be tested for need by Central authorisation administrator (SA), and can only be used for the documented purpose.

5.1.1.1.3 If an employee also is registered as customer (TeleBank, Nettbank etc.) for private relations, the user must in this relation have a UserID in accordance with customer standard. An employee UserID cannot be used in private customer relations.

5.1.2.1.1 ✓ The following systems requirements apply to passwords:

1.	Password length	: Minimum 6 - Maximum 8 characters.
2.	Password content|	: Must contain numbers and letters
3.	Password quality	: Passwords similar to user identity is not permitted
4.	History	:The past 5 passwords cannot be reused
5.	Change of password	:Forced changed after maximum 60 days usage
6.	Voluntary change	:Possibility to change when wanted
7.	Change notice	: Notice 7 days before expire
8.	Password verification	: New pwds must be verified by entering it twice, before the change takes place
9.	No. of wrong attempts	: The UserID is locked after the 5th wrong attempt
10.	Protection	: No display on screen or printout
11.	Storage	: Must be encrypted during storage and transfer

5.1.2.1.2 Password requirements must be handled by the security- or operational system both on central and distributed platforms, and must not be handled by isolated program or subsystems.

5.1.2.1.3 ✓ Special UserIDs in programs etc must have a maximum length of 8 characters and must be changed at least annually. The password must be difficult to guess and must be well (RED) protected during network transport and use.

5.1.3.1.1 ✓ UserID, which has not been used over a 3-month period, must be removed from (all) platforms and applications the user might have access to.

200 requirements

Security analysis

Single Sign-On fra Troll-plattformen blir videreført i SDP og skal benyttes for å redusere passord-byrden for brukerne. Hvis dette ikke er mulig, skal en utnytte at bruker allerede er pålogget NT. Ved å koble det nye IT-systemet til NT, slipper brukeren ny pålogging. Hvis IT-systemet er en intern E-applikasjon i DnB NORs E-arkitektur ("DnB RZ"), skal mekanismer for Single Sign-On gjennom intern DMZ benyttes. (Kundens sikkerhetsløsninger skal ikke benyttes av interne ansatte.)

Brukerstøtte (18700) og EDB IT Drift IT Service (23100) skal – som før - ha 1.linje support for administrasjon av passord. Dette vil bli samordnet senere.

Det vil bli foretatt en harmonisering av krav til passord i alle systemer i DnB NOR, slik at brukeren kan ha samme passord i de systemer som holder sikkerhetsnivået i KKIS.

S19 Hvilken desentral plattform skal brukerne benytte ved tilgang til IT-systemet? *(kryss av)*

Troll og/eller FDP	□
SDP (Samordnet Desentral Plattform)	□
Annet (spesifiser):	

S20 Vil brukerne få ny pålogging utover pålogging til NT, Trolls Single Sign-On løsning og/eller ACF2?

Nei □ ⇩ Vennligst beskriv hvordan Single Sign-On oppnås:

Ja □ ⇩ Vennligst besvar følgende tilleggsspørsmål:

1.	Hvilke plattformer og/eller databaser skal bruker logge seg på til?
2.	Er det gjennomgått med leverandør/systemeier å eliminere/forenkle påloggingen[16]?
3.	Er ekstra pålogging konsekvensvurdert[17]?
4.	Beskriv hvilken brukerID som benyttes.
5.	Beskriv avvik fra systemkrav for passord, ref. KKIS kapittel 5.1.2.1.1.
6.	Beskriv hvordan brukerID og passord oppbevares sikkert i denne løsningen.
7.	Beskriv hvordan sikkerhetslogging blir ivaretatt, ref. KKIS kapittel 6.5.1.1.1 og 6.5.1.1.2.
8.	Hvilket verktøy benyttes for å administrere brukere?
9.	Hvilken prosess gjelder for administrasjon av brukere?
10.	Hvilken instans vil foretå eventuelt behov for utdeling av passord/løse opp i passordproblemer[18]?
1.	
2.	

60 questions &answ

Security metrics

Security Status at delivery

Research Question

Figure 2 The relations that lead to secure systems

1.2 Justification, motivation and benefits

The system development area in the Bank has an annual budget of > 70 mill Euro and E-commerce has a steadily increased share of this budget. To manage the development of secure solutions is of great importance to risk management in the Bank.

The planned research and the resulting security metric should give the Bank valuable insight into the relations between the security framework that the project is supposed to comply to, the Security analysis with its dialogue, questions and answers and the security facts measured at delivery.

The security metric will serve different purposes:

- To measure the security status of the system
- To measure or indicate the effect of the Security process and analysis

The main goal is to manage risk associated with loss of Confidentiality, Integrity and Availability. Analysis of the areas of non-compliance, the associated risk and the root cause will be important parts of the risk management.

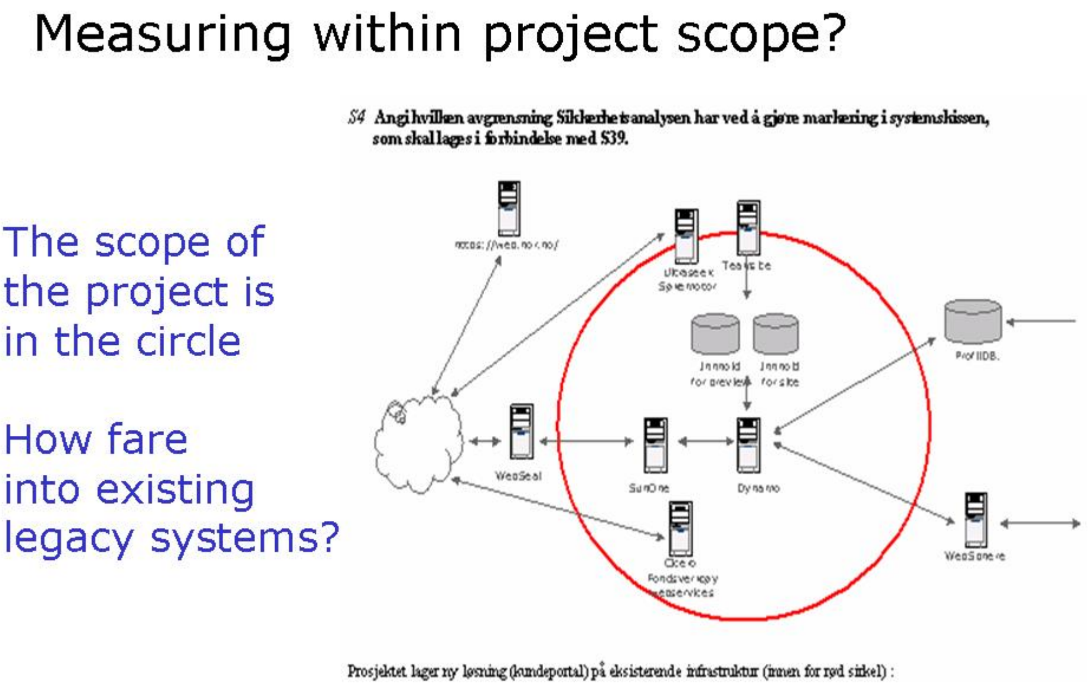
1.3 Research question

The research question is ho*w to define a security metric that measures the security status of a new system at delivery in an objective and concise manner*.

The term *security status* can be defined from different points of view:

- The degree of compliance to the advice of solutions and requirements included in the Security analysis of the system
- The degree of compliance to (a subset of) the Bank's Security requirements (BSR)
- To explain the security status and area of non-compliance in terms of the business need for Confidentiality, Integrity and Availability

The scope of the *security status* must be decided in the thesis from a reasonable combination of these points of view.



Measuring within project scope?

The scope of the project is in the circle

How fare into existing legacy systems?

S4 **Angi hvilken avgrensning Sikkerhetsanalysen har ved å gjøre markering i systemskissen, som skal lages i forbindelse med S39.**

Prosjektet lager ny løsning (kundeportal) på eksisterende infrastruktur (innen for rød sirkel) :

Figure 3 Measuring within project scope

A development project will normally deliver a new system that will be integrated with the existing systems. The project will define a scope in terms of deliverables and which part of system chain it is responsible to secure.

If we measure security elements outside the *project scope*, then the Project manager may not be held accountable. The security implications outside of this project scope may be real, but challenging to address inside the project.

An example: a project will use *an existing* Message Queuing solution to integrate to the backend system, but this solution has no encryption or authentication. The metric should reveal that the encryption and authentication is missing. But as the project did not establish the channel, it is an open discussion if the project is responsible or if this should be addressed to the Owner of the existing solution.

The term *at delivery* can be defined as the milestone in the project where all security decisions are implemented and were facts can be verified. Preferably this will be before the system is going live so security problems may be known before they pose a risk.

2 Review of previous work

The main focus of literature review is on designing of the security metrics and on measuring.

2.1 Theory on security metrics

A great deal of research has been conducted to develop theory and methods of measurement or designing metrics for different purposes. On security metrics, the amount of work is still extensive, but the field is immature. There is no generally recognized metric or method to build on, but there are many different approaches debated.

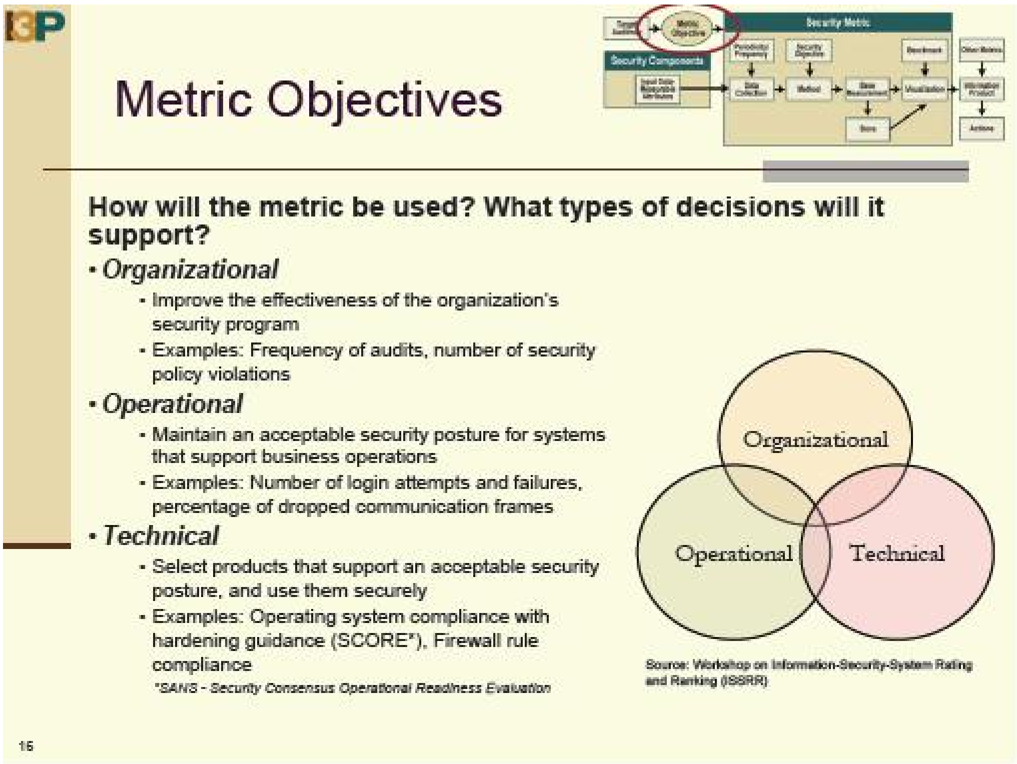
In designing a security metric, one has to be very conscious of the fact that a metric simplifies a complex technical and human situation down to some numbers. McHugh [13] and McCallam [14] are sceptical of the side effects of such simplification and the lack of scientific proof that the evaluated metrics has validity. Yee [15] concludes that a multi-faceted or multi-dimensional security measure is needed.

The Security metrics guide [4] from NIST[1] gives guidance on how an organization, through the use of metrics, identifies the adequacy of security controls, policies and procedures, with a sample metrics in the addendum. The NIST security program maturity with metrics and methods has been improved by KITH[2] to be used in the health care sector in Norway [16]. FIPS has proposed classification of security metrics [27]. Vaughn et al. [23] proposes taxonomy for Assurance measures and metrics.

Payne [6] focuses on the properties of a good metric and describes how metrics can be used to develop the security awareness in the organization. Wang [7] describes the importance of a clear definition of what and how to measure. Henning [24] also proposes a definition of security metrics. Jelen [26] states that a good metric must be “SMART”: Specified, Measurable, Attainable, Repeatable, and Time independent. The paper Assurance measures and metrics [9] by Vaughn et al. defines how to express confidence in security countermeasures. Stoddard et al. [22] reports in “Security metrics overview” on a research project which defines a framework for security metrics. A sample from the report is shown in the following figure.

[1] National Institute of Standards and technology, USA

[2] Norwegian Centre for Informatics in Health and Social Care



Metric Objectives

How will the metric be used? What types of decisions will it support?

- *Organizational*
  - Improve the effectiveness of the organization's security program
  - Examples: Frequency of audits, number of security policy violations
- *Operational*
  - Maintain an acceptable security posture for systems that support business operations
  - Examples: Number of login attempts and failures, percentage of dropped communication frames
- *Technical*
  - Select products that support an acceptable security posture, and use them securely
  - Examples: Operating system compliance with hardening guidance (SCORE*), Firewall rule compliance

*SANS - Security Consensus Operational Readiness Evaluation

Source: Workshop on Information-Security-System Rating and Ranking (ISSRR)

16

Figure 4 From "A framework for Security Metrics"

Frost [5] defines a general framework for measuring to a Balance scorecard and Snekkenes [28] takes this concept further to a method for security metric design. Bakås et al. [8] has proposed security metrics related to SLA[3] in outsourced IT operations. The project "Security Reporting" [11] explains how security indicators presented to management can trigger decisions on security controls in order to reduce vulnerability in an infrastructure. The ongoing project "BAS5 Critical Information Infrastructure Protection" [12] is developing a method to prioritize a list of proposed security controls from aspects like cost efficiency.

Bakås [34] has also proposed a "Process for measuring the information security level".

2.2 Measuring Security in practice

Law or regulation requires risk analyses. As this thesis is designing a metric for compliance to

[3] Service Level Agreement

the Bank’s BSR, it may be more adequate to apply a risk analysis method (i.e. NS 5814 [25]) on the areas of non-compliance to enlighten the associated risk.

The Financial supervisory authority of Norway (Kredittilsynet) has issued general IT governance requirements to the banks, and has an inspection programme with a checklist to check for compliance. The requirements are on a very high level and must be interpreted to be measurable. The checklists are more detailed but are not available outside the authority.

Checklists like Windows Security checklist [17] can be viewed as a form of metric, which enlightens where the security of a system is non compliant to an ideal list of security recommendations. Again, one has to analyse the risk of the areas of non-compliance. The bulk of such checklists are aimed at securing technical platforms and infrastructure, and not at securing applications in a business context.

In a larger scale one could regard the Bank’s security requirements as a ”checklist”, and this thesis tries to some extent to do that as a part of the metric.

The bank has outsourced its IT Operations, and as a part of the contract, a security agreement with SLA on security issues like Firewalls, IDS and IRT[4] was established.

To be able to measure compliance to the agreement and SLAs, a security metric was developed. The metric was evaluated as an assignment [3] in the course IMT 4111 Security Metrics at GUC. The experience in designing the metric and evaluating it afterwards have been valuable in this MSc thesis.

ISF[5] has established the ”Standard Of Good Practice” SOGP [2] and the accompanying ”Information Security Status Survey”. The Survey is only available to the members of ISF and it measures compliance to SOGP and ISO 17799. In addition it offers a benchmark comparison to the other members of ISF on the total or by business sector. The Survey consists of 5 types of questionnaires that cover different aspects like System Development or Critical Business Application.

As there are more than 100 members participating in the Survey, ISF can issue an opinion on security matters on behalf of the members within reasonable confidence levels. In analysing the Survey database across all members, ISF has defined some Critical success factors and Benchmark issues that lead to a lower rate of security incidents.

[4] IDS – Intrusion Detection System, IRT – Incident Response Team

[5] Information Security Forum [2]

ISF has also developed a simpler and more focused metric called “Security Health Check”.

ISF runs a project to develop a Meta standard that ties ISO 17799[1], ISF SOGP [2], CobiT [39]and other standards together by a common structure and cross reference tables. The Survey, the Health check and other metrics will be used to measure compliance against any of them.

As the Bank is a member of ISF and the Author has experience in using ISF methods, the security metric from this MSc thesis has also been inspired by topics and methods from ISF.

3 Summary of claimed contributions

The new knowledge of general interest is a valid and reliable prototype security metric built on the theoretical principles and practical experience from chapter 2 *Review of previous work*, and the documented process of designing it.

The Bank receives a prototype security metric for a specific area of the Bank and some pilot measurements.

The research and evaluation should also give the Bank valuable insight in the relations between the security framework that the project is supposed to comply to, the Security analysis with its dialogue, questions and answers and the security facts measured at delivery.

Security metrics is an immature field of experience and few real world examples exists. It is important to demonstrate the security results of security work, effort and investment, but this is rarely done.

We hope that this MSc thesis can provide knowledge and real world examples as an inspiration to others.

4 Choice of methods

Security metrics is an immature field and there is no accepted method that is supported by evidence of its correctness. Whether this thesis delivers a valid and reliable metric of general interest will depend on the research design. The approach has been to combine the theoretical principles from chapter 2 *Review of previous work* with practical experience and the need of a metric for a specific field of the Bank. The resulting metric must represent new knowledge of general interest, and must also be suitable for the Bank’s need.

Both qualitative and quantitative methods will be used and a Mixed method approach [21] seems necessary.

4.1 The Author's role

The Author has been the main author of the Baseline Security Requirements document (BSR) and a strong contributor to the Security analysis, which constitute the basis for the metric. There may be a risk that the Author may be biased and may try to design a metric that is self-evident, by giving unconscious credit to previous work or avoiding weak areas.

To compensate for this the Author has arranged for a Reference group with internal experts in the field of System developments and security to oversee and approve the selection of parameters and the development of the metric.

The Reference group should:

- Observe and correct a possible bias by the Author
- Ensure a practical metric for the Bank
- Ensure management support for implementation of the metric after the MSc thesis

Though this can result in a useful metric to the Bank, there is a risk that the proprietary setting – from a scientific point of view - may lead to a “home grown *suggestion* of a metric” instead of achieving new general knowledge on metrics that are understood and approved by independent researchers.

To compensate for this the Author has arranged for independent reviews. The supervisor will be the main source for this but we will also use Peer review and seek a second opinion from independent researchers.

4.2 To define a framework for the security metric

The framework should describe:

- How the security status should be presented
- How the metric and analysis can indicate the effect of the Security process and analysis
- How the metric can enlighten which area and topics in the process and analysis need improvement
- How validity and reliability are achieved

It is expected that the final metric mainly will consist of integer scales as the prototype does.

Examples of topics or features:

- Is Single sign-on implemented in the system?
  The scale of this metric can be binary: 1=Yes, 0=No but we may need a scale for evaluating partial compliance
- Has the project verified the audit trail of the transactions?
  The scale of this metric may be to assess the percentage of verification: 0, 25, 50, 75 or 100 and we could code this as a number between 0-4
  A comment field may explain the areas or aspects not verified

4.2.1 ISF's metrics

As mentioned in chapter 2 *Review of previous work*, the Bank uses ISF's security metrics on other fields, and it is natural to use input from ISF's metrics and methods in the final metric. As debated under section 8.7 *Ethical and legal considerations* this introduces a need to balance the ISF copyright against a public MSc thesis.

We therefore use ISF metrics as an inspiration and evaluate the methods used, but we design a metric that is based on its own scientific principles. We have also arranged for a review of the MSc report by a member of the ISF management team in order to ensure that balance.

There are at least 2 ISF metrics of special interest:

- The Survey which contains 5 questionnaires of approx 500 questions each
- The Security Health check, which contains < 100 questions in the relevant sections

We use the method Content analysis [18] to describe the topics that are covered in the ISF metrics and use a Semi structured interview [18] in describing what criteria were used in the selection of the 100 questions in the Health check out of 2500 questions in the Survey. We interviewed the ISF Management responsible for the metrics.

ISF has analysed the Survey database across all members, and has found some Critical success factors and Benchmark issues that leads to a lower rate of security incidents. We use Content analysis to see the value of these factors and issues to the Bank in designing the metric.

ISF runs a project to propose a Meta standard that ties different standards like ISO 17799, ISF SOGP, CobiT and others together and cross referenced to use the Survey and the Health check to measure compliance against any of them. As the Bank now is rewriting its Security framework to the structure of ISO 17799 and SOGP, the structure of the Meta standard can be natural to base this thesis's metric on.

We perform a Content Analysis of the ISF Meta standard documents to describe the common structure and categories that ISF proposes for this Meta standard and evaluate them for use in this thesis.

4.2.2 Reliability

A general problem with ISF metrics is that they are based on self-assessment, and there is no clear description of which ”proof of implementation” is needed. The Survey imposes a workload due to several hundreds of questions, which may lead to quicker and less thorough assessments. This may lead to a systematic bias or random error that causes reliability problems.

The metrics from this thesis should state how the user can assure that each value in the metric is correctly assessed – ".. in an objective and concise manner". The ultimate "seeing is believing" will generate more work - and maybe an unrealistic effort of testing – to establish the proof we ask for.

Generally it can be helpful to describe (some of) the metrics in the form recommended in NIST Sample metrics [4], by describing topics like "implementation evidence", "algorithm" etc in order to increase the precision and thereby reduce errors caused by the human factor.

Using different persons to measure the same system and analyse the root cause of the differences in measurement can test the reliability of the metric.

We need to balance the scientific need for accuracy and the business need for a manageable workload of measuring.

A partial solution to the reliability problem with security metrics is to use the same person or a small group of trained people as supervisors when the metric is used. This can ensure a consistent understanding and use of the metric, reduce the need for lengthy, precise instructions to the user and reduce the possibility of bias.

For the Bank, it may be natural to use dedicated security consultants to supervise the use of the metric and to quality assure the measurements. Existing tools like Security analysis, Risk analysis and others are already conducted assisted by dedicated consultants.

4.2.3 Summary of methods

The framework and requirements for the metric has been described by the following methods:

- By studying Previous work within the context of the research question and define the existing scientific principles for the metric.
- By conducting a qualitative Content analysis of the 60 questions of the Security analysis and compare them with the 200 Security Requirements in order to establish an overview of the security topics covered
- By conducting a Content analysis to describe the topics in the ISF metrics and do a qualitative Semi structured interview [18] in describing the selection criterions used in the Health check. We interviewed the ISF Management responsible for the metrics
- By conducting a Content analysis on ISF documents that describe the factors and issues that reduce the frequency of security incidents and assess the relevance to the Bank
- By conducting a Content analysis and a Semi structured interview in describing what common structure and categories that ISF proposes in the Meta standard. We interviewed the ISF Management responsible for the project

4.3 To define the topics to be measured in the Security status

The main challenge has been to define which topics that should be measured. As stated earlier there should be a reasonable combination of different aspects that would give a fair content validity of the security metric and at the same time accountability.

In the Project risk analysis that was conducted in the planning of the MSc thesis, the highest risk found was that the scope and workload of the thesis may grow too big to be completed within the given timeframe. To avoid this situation, there was a need to prioritize the aspects and - if necessary - to limit the scope accordingly.

This prioritization has been used in designing the prototype metric:

1. The degree of compliance to the advice and requirements included in the Security analysis for the system (60 questions)
2. The degree of compliance to (a subset of) the Bank's BSR
   (uncovered parts of 200 requirements)
3. To explain the security deviations that the status reveals in light of the business need for CIA[6] from the Risk analysis

The main purpose of this thesis was to develop a metric to measure the effect of the Security analysis. If the metric needs further improvement to give a broader coverage of aspects, this could be done after the MSc thesis is finished.

On the other hand, to represent knowledge of general interest, the content validity and generalization of the security metric is assessed in the section *How to generalize the metric* in the final chapters of the report.

The topics to be measured in the metric are described by the following methods:

- By analysing and structuring the findings from the previous step to present the outline of the metric and a list of possible categories and topics to be measured
- By conducting a Semi structured interview with relevant managers and Reference group in the Bank to describe the business requirements for the metric. The questions and topics in the interview is influenced by the findings in the previous steps
- To summarize the resulting metric from the steps conducted, and debate them in the Reference group and with independent researchers

4.4 To test, improve and use the metric

We have used quantitative Descriptive analysis [18] to test the metric.

In section *Further work*, we have recommended to test and retest the same system with different users to indicate reliability.

In analysing the measured result, one should use quantitative analysis of the test and retest combined with qualitative analysis to find improvement areas and root cause of errors and bias.

[6] Confidentiality, Integrity, Availability

4.5 General MSc thesis

To seek quality in all aspects of the tasks performed, we have used methods from Leedy [18] and Stene [19].

5 Defining a framework for the metric

It is useful to repeat the assignment: to develop a security metric to measure the security status of an IT system when it is delivered from the development process.

The primary function of the metric is to:

- Document the security status for risk management and compliance purposes
- Measure the effect of the security process and indicate areas of improvement

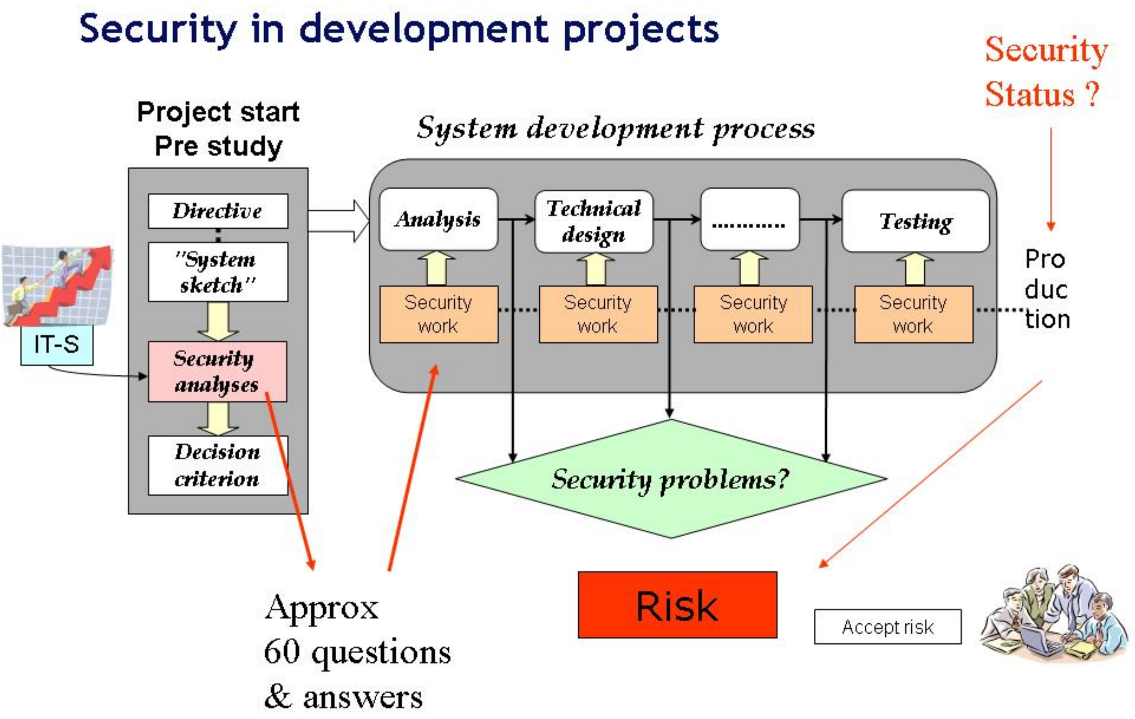


Figure 5 Security in development projects

The section: *Previous work* defines the scientific basis for a security metric. The most important and suitable references and applications when designing this metric are:

- To develop the metric by the method described in Security metrics course[28]
- To base the metric on the principles in NIST 800-55 [4] combined with the principles of the ISF metrics

The rest of the previous work described will be referenced when relevant.

5.1 A method for security metric design

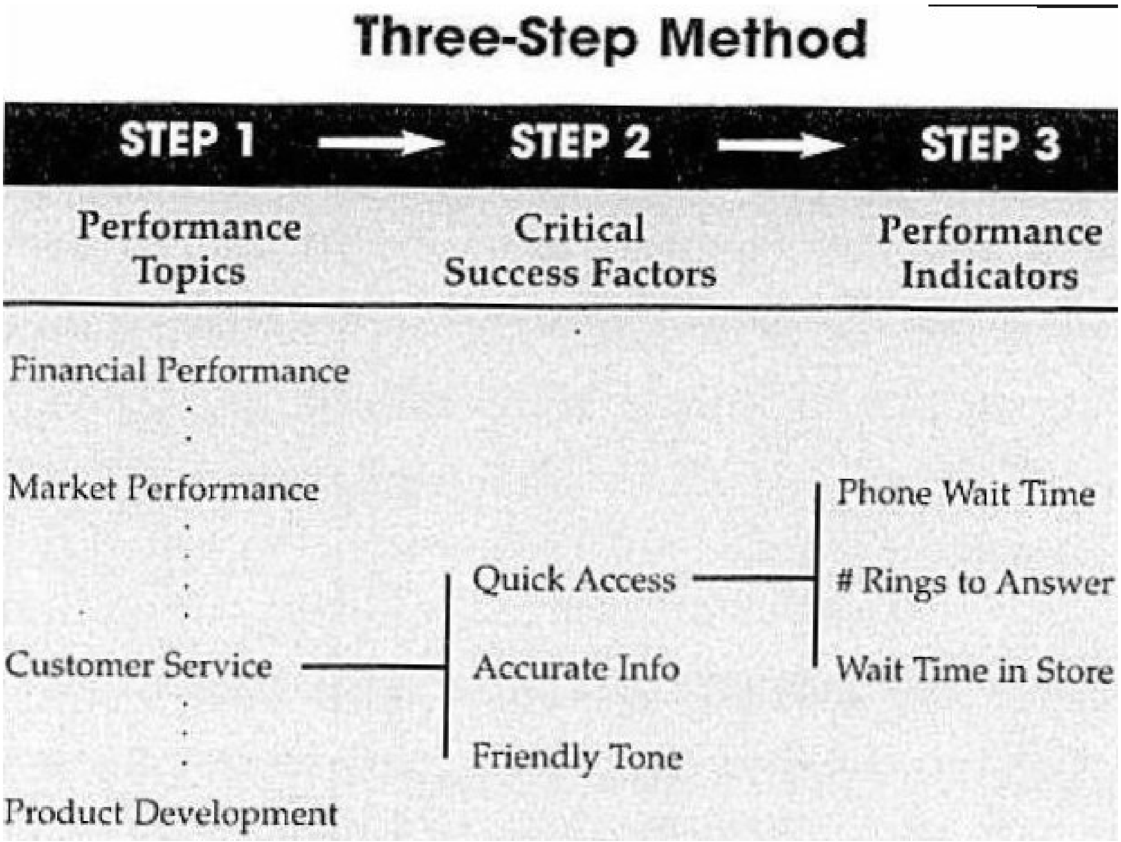


Figure 6 Three-step method [5]

The lecture [28] presents a three-step and top down method for developing a metric:

1. Identifying the Performance topics

Typical for security: Secure systems to protect Confidentiality, Integrity, and Availability

2 Identifying the Critical success factors for each Performance topic

Typical: existence of a clear, known, agreed and understood definition of the performance topics and how to achieve the performance

3 Identifying Performance indicators for each success factor

Typical: indications that the definition of performance topics are clear, well known, agreed and understood so the user knows what is expected and can contribute to success and measurement with reliability

The lecture also makes important discussions on:

- Identifying who we measure for: the stakeholders, and why they should measure or use the results. This is important to design the metric to match their needs, and assure their support

- “Clear line of sight”: the metric must demonstrate a clear connection between the Stakeholders' decisions and actions in the project and the results measured to provide accountability
- The effect of measuring: "You become what you measure"

These topics are applied as a starting point for a framework for the metric.

5.1.1 The three-step method

The method makes the user establish a clear link between the business need for risk management through security measures down to how each element in the metric gives indication of how successful the performance is. As such it assists in describing the business function of the metric.

Performance topics

The main reason for the Bank to have a security focus is to manage business risk. IT related risks are an important part of operational risk with Internet banking. The IT related risks are mitigated by security measures to maintain the necessary confidentiality, integrity, and availability of business data.

The main performance topic for this metric is to make the user aware of weaknesses in the security measures that can lead to loss of confidentiality, integrity, or availability and to manage the associated business risk.

Critical success factors for each topic

As described in section 1.1 *Problem description*, the Bank has a security process and security requirements that support confidentiality, integrity and availability. The development projects must comply with this and the Security analysis supports the implementation process. The Bank therefore wants to develop a security metric to measure the areas of non-compliance of the system when it is delivered from the development process.

The critical success factors for this metric are the existence – in the Bank - of a clear, known and understood security requirements document (BSR), security process and a Security analysis to support this process.

Performance indicators for each success factor

The performance indicators for each success factor for this metric are the compliance to the security requirements and the security process. (Areas of non compliance indicates lack of success)

Analysis of the areas of non-compliance and the root cause may lead to different conclusions:

- To enforce compliance to support the success of confidentiality, integrity, or availability and to mitigate risk
- To accept risk of the area of non compliance and the associated risk of a breach of confidentiality, integrity, or availability
- To improve the clarity, knowledge and understanding of the security requirements document (BSR), security process and Security analysis

5.1.2 Who we measure for: the stakeholders

As described, we want to measure the security status defined as the compliance to the Bank's BSR and to the security process. Who needs these measurements and for what?

The lecture [28] defines the stakeholders as roles that will influence – or will be influenced by - the success or failure of our goal, in this context: compliance to security requirements in order to reduce risk.

A short analysis of the stakeholders relevant for this metric:

- The project manager/Business developer
- The system owner/Business owner
- Management

The Project manager/Business developer

The project manager and the business developer come in pair where the first is responsible for the projects delivery according to agreed requirements and project description and the second is responsible for the business approval of the requirements and project description and for ensuring business success when the system is delivered.

Security is a natural part of this process and the Security analysis is used to define the relevant security requirements and thereby the security solutions to achieve a risk level that is accepted by the business.

But, when we look at the focus and attitude of these roles we see a little different picture. Project managers and business developers are chosen because of their proven ability to invent new processes and IT systems to support them. They are skilled and trained to:

- Deliver on time and on budget
- Simplify, reduce the scope and complexity of the project, only focus on the essentials to deliver what is the essence and not “nice to have”
- To fight the organisations resistance to change and risk of change
- Avoid describing problems and convert them to “challenges and opportunities”

Ideal issues like security, risk, “quality”, documentation and operational issues after delivery will probably never be in primary focus for these roles and they will normally look for the minimal solution in these areas. The business managers express a need for rapid development and may criticise the IT development for being slow and expensive. From a business point of view, one would perceive a choice between two non-ideal deliveries:

- A “prototype” system with security solutions based on compromises but finished on time and budget to enable the business to penetrate the market without lagging behind competitors
    - “The rest can be dealt with in later versions if the market share increase”
- An ideal and total solution secure and planned for increase in business volume,
  but with increased development budget, longer time to market, greater complexity and maybe running late.
    - “The money may be wasted if the concept does not get accepted in the market”

When we look at the increase in customers of electronic banking from 1997 until today - >1 mill - it was not easy to foresee and plan all security aspects at the first "prototype" of a banking service channel. If we combine this fact with the perception that these roles may have that the security consultant is risk adverse and is trying to bring in risk and security aspects that are not yet recognized as real or necessary, there is a risk of miscommunication.

For these roles the Security analysis is an established tool in the Bank, but they will probably not be a primary driver for a new security metric that may increase the security effort and put utterly focus on the security compromises that they have made.

But with no doubt, they are the most important roles for success of security – or failure - because they have the funding, recourses and responsibility to secure the system as they build it. The metric will enlighten their security performance and give feedback to improve this performance.

An assumption is that the introduction of a security measurement at delivery may improve security by itself. The assumption is that both the security status and the fact that others will assess the decisions and compromises may contribute to this improvement.

The System owner/Business owner

The System owner and Business owner also come in pair where the first is responsible for the IT-system and its maintenance and operation according to agreements or SLA and the second is responsible for the business process and business operations of the system. The development project delivers to these roles.

They have analogue roles and responsibility with the Project manager and the Business developer, but with a major distinction: they are responsible for the day-to-day operation when the system fails or security problems occur.

So, when we look at the focus and attitude of these roles we see a different picture from the previous. System owners and Business owners are chosen because of their proven ability to operate business processes and IT systems to support them. They are skilled and trained to:

- Stabilize the business process and fine tune it
- Keep the system running and prevent operational and security events
- Analyse the total of the system – which often consist of deliveries from several different partial projects
- Describe problems and risk of security, robustness and growth and solve them in a maintenance plan

As these roles may not be participating in the project, they are not the most important roles for achieving success of security in the delivered system, but are the main users of the same security and will inherit responsibility for the weaknesses in the security status at the time of delivery.

Their main interest in the metric will be to document the security status at delivery to make them aware of what operational risk they inherit.

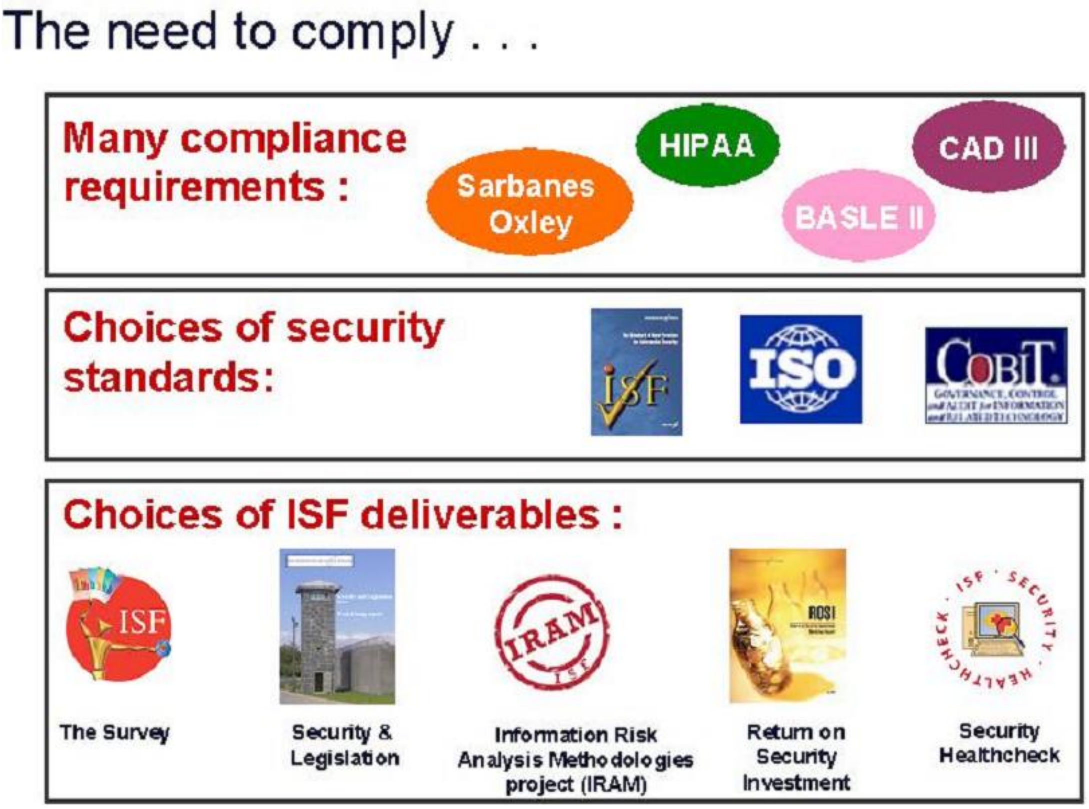
Management

Management as a stakeholder in the metric can be illustrated from different roles:

- Top management
- Management of System development
- Head of IT-Security

Top management

After many years of public and global de-regulation, we now see trends of re-regulation. The scandals of Enron and others have made the politicians develop new laws [30] like the American Sarbanes-Oxley [31]. The intention is to place the responsibility on the Board and CEO to know facts of risk and operation and to report this fairly and honestly to the market. The reporting must cover the whole range of financial, business and operational risks including Information security related risk and the board and CEO are personally liable for the correctness.



The need to comply . . .

Many compliance requirements :

Sarbanes Oxley

HIPAA

BASLE II

CAD III

Choices of security standards:

ISF

ISO

COBIT

Choices of ISF deliverables :

The Survey

Security & Legislation

Information Risk Analysis Methodologies project (IRAM)

Return on Security Investment

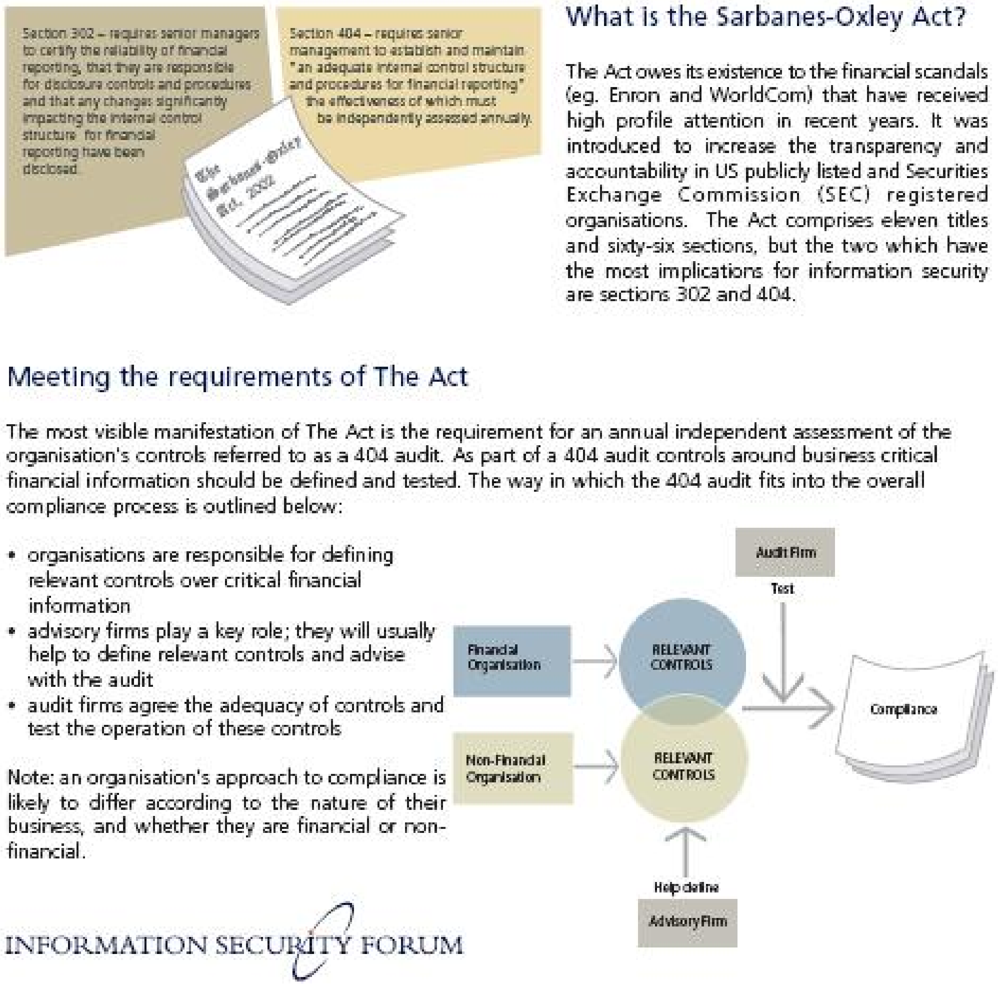
Security Healthcheck

Figure 7 The need to comply (ISF)

An effect of this is that the words *compliance* and *risk management* have become more important to managers in order to reduce personal liability. Tools like security metrics that can assist the top management in verifying compliance and associated risk of non-compliance are welcomed.

Top management will probably not use the metric directly, but may use a Risk management staff and Risk managers in different sectors to gather such information and will endorse any effective way of improving this process.

Top Management will use the data from the metric, but can only indirectly contribute to security success in each project by – visibly - supporting the security focus, processes and priority to other aspects. This is visualized in the ISF report: Sarbanes-Oxley – Implications for information security [29].



Section 302 – requires senior managers to certify the reliability of financial reporting, that they are responsible for disclosure controls and procedures and that any changes significantly impacting the internal control structure for financial reporting have been disclosed.

Section 404 – requires senior management to establish and maintain "an adequate internal control structure and procedures for financial reporting" the effectiveness of which must be independently assessed annually.

What is the Sarbanes-Oxley Act?

The Act owes its existence to the financial scandals (eg. Enron and WorldCom) that have received high profile attention in recent years. It was introduced to increase the transparency and accountability in US publicly listed and Securities Exchange Commission (SEC) registered organisations. The Act comprises eleven titles and sixty-six sections, but the two which have the most implications for information security are sections 302 and 404.

Meeting the requirements of The Act

The most visible manifestation of The Act is the requirement for an annual independent assessment of the organisation's controls referred to as a 404 audit. As part of a 404 audit controls around business critical financial information should be defined and tested. The way in which the 404 audit fits into the overall compliance process is outlined below:

- organisations are responsible for defining relevant controls over critical financial information
- advisory firms play a key role; they will usually help to define relevant controls and advise with the audit
- audit firms agree the adequacy of controls and test the operation of these controls

Note: an organisation's approach to compliance is likely to differ according to the nature of their business, and whether they are financial or non-financial.

INFORMATION SECURITY FORUM

Figure 8 ISF: Sarbanes-Oxley - Implications for Information Security

Management of System development

The management of System development is responsible for annual budget of more than 70 mill. Euro and deliver > 60 development projects pr year.

To control this large production, system development processes are defined with roles and responsibilities that include security and risk management. The management does not want to be involved in details of each project as this is delegated to the project manager and the business developer of each project as described earlier.

The managers need indications of systematic deviations from the process and security standards that can assist them in improving performance in the overall production. The indications must be supported by examples that illustrate the deviation and that indicates the root cause:

- Flaws in the security and risk accept process in projects or escalation to management
- Flaws in the security requirements, the security solutions or the description and understanding of them
- Flaws in Personal accountability, biased focus or security motivation

The metric from each project can form a basis for statistics that can indicate systematic deviations and to support them by examples. The root cause may have to be found by separate analysis and interviews of participating roles.

The management of system development can directly and indirectly influence the success or failure of security in each project by actively supporting the processes, motivate and train for security and react on signals of flaws and direct escalations.

The management of system development is also participating in the top managements' Risk management process by collecting and reporting facts and evaluations on risks related to IT and can use the metric as a part of the data collection.

Head of IT-Security

The head of IT-Security is responsible for:

- Defining the security process and tools to support it (I.e. Security analysis and metric)
- Defining security requirements and approved/recommended security solutions
- Supporting the projects by skilled Security consultants that have adequate skills in both security and process

In this context IT Security is a part of the system Development value chain and has parallel needs to head of Systems development in improving performance of the delivered services.

The head of IT-Security is also participating in the top managements' Risk management process by collecting and reporting facts and evaluations on risks related to IT and can use the metric as a part of the data collection.

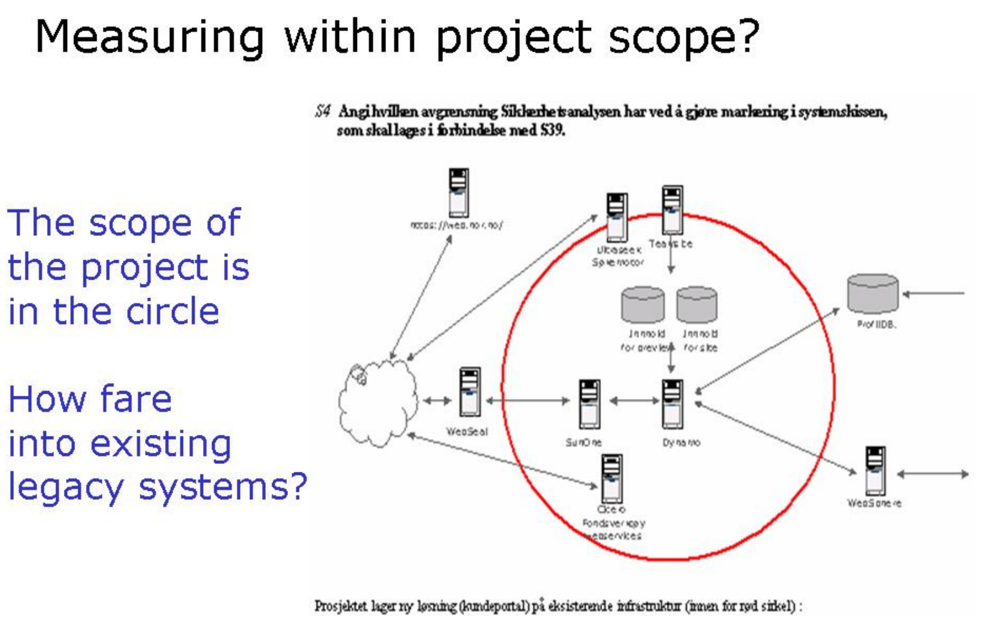
The head of IT-security can indirectly influence the success or failure of security in each project by actively improving and supporting the processes, motivate and train for security and can directly influence the security level by escalating risk to higher management.

A summary

STAKEHOLDER	PURPOSE OF METRIC
Project manager / Business developer	Primary responsible for the security at delivery. To document security status and learn from their own performance.
System owner / Business owner	To know the security status when they take over the responsibility from development.
Top management	To manage risk and to quality assure facts before they report externally to reduce their personal liability.
Management of System development	To collect statistics to see trends of systematic problems and flaws in development processes that lead to security problems.
Head of IT Security	To assist top management in managing risk and to manage and improve the security process and deliverables (i.e. Security analyses).

5.1.3 "Clear line of sight" and accountability

The metric must demonstrate a clear connection between the Stakeholders decisions, actions and responsibility in the project and the results measured. This will make it easier for the major stakeholder to accept accountability for the result and to be able to learn and improve by the feedback given in the metric. An example that demonstrates a possible *unclear line of sight*:



Measuring within project scope?

S4 Angi hvilken avgrensning Sikkerhetsanalysen har ved å gjøre markering i systemskissen, som skal lages i forbindelse med S39.

The scope of the project is in the circle

How fare into existing legacy systems?

Prosjektet lager ny løsning (kundeportal) på eksisterende infrastruktur (innen for rød sirkel) :

Figure 9 Measuring within project scope

A development project will normally deliver a new system that will be integrated with the existing systems. The project will define a scope in terms of deliverables and which part of the system chain it is responsible to secure.

If we measure security elements outside the *project scope*, then the Project manager may not be held accountable. The security implications outside of this project scope may be real, but challenging to address inside the project.

An example: a project will use *an existing* Message Queuing solution to integrate to the backend system, but this solution has no encryption or authentication. The metric should reveal that the encryption and authentication is missing. But as the project did not establish the channel, it is an open discussion if the project is responsible or if this should be addressed to the Owner of the existing solution.

Another example of *clear line of sight* is defining which requirements from BSR that is relevant to system development projects and therefore is within the responsibility of the project. This topic is described in the section: *The content analysis of the Bank's security requirements*.

“Clear line of sight” and accountability is an important aspect in designing the metric and must be verified with the stakeholders.

5.1.4 The effect of measuring - "You become what you measure"

The lecture [28] warns of the effect of measuring. On one hand, one cannot measure everything, a selection and prioritisation is needed. On the other hand – if a project manager knows that the security performance will be evaluated by a metric, then management has demonstrated that *the security topics in the metric* are more important then other security topics.

Another expression illustrating the same point is: "You measure what you treasure".

But overall – without a type of follow up tools like Security analysis and metric, the security field will loose in the battle for attention and will not demonstrate results.

5.1.5 Other issues from the lecture [28]

Two metric categories are defined:

- Primary metrics
  - Performance observable by parties external to the organisation
- Advanced metrics
  - Focus on internal work process and capabilities

According to this classification, this metric is an “advanced metric” in a sense that it is not enforced or designed by an external party, but it is required by the Bank to focus and improve internal security performance with the intention to manage operational risk.

If the main reason for making it was to demonstrate compliance to – say – external auditors, then it would have been a primary metric.

This issue is debated in the section "The Authors personal experience"

5.2 The principles given in NIST Special Publications 800-55

NIST SP 800-55 Security Metrics Guide for Information Technology Systems [4] is a well-respected and referenced publication regarding measuring security. As NIST is a US government office, the context and reference environment is public sector and the effort to comply with public security regulations.

The guide defines a metric development process with metrics considerations and success factors that deals with the same type of issues as in the previous section, but in a more governmental context. It builds its content on a series of NIST 800-xx documents.

The guide [4] has 2 very relevant areas that are used in the framework for the metric:

- Security program maturity
- Metric detail form

5.2.1 Security program maturity

A reference is made in the metrics guide to a Security program maturity concept and this is presented in context of types of measurement and levels of maturity.

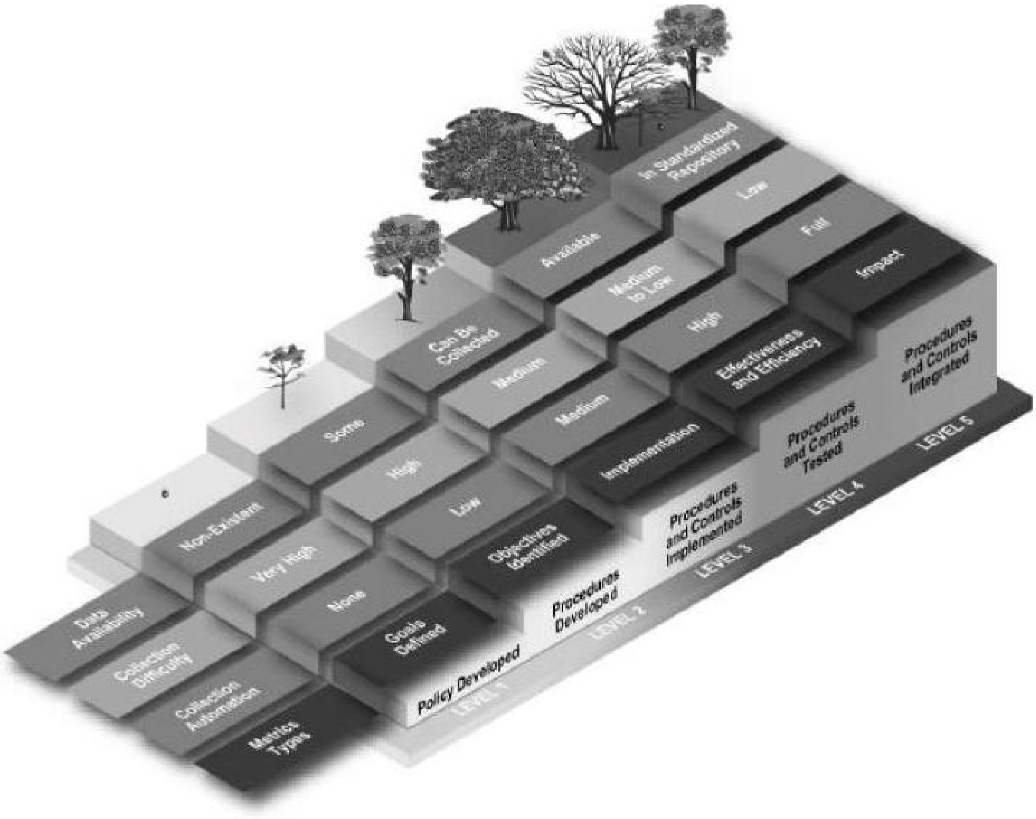


Figure 10 NIST: Security program maturity and types of measurement

Essentially, it states that the types of measurement and metric one want to define must be in sync with ones business security program maturity. If one does not take this into account one may not be able to obtain the measurement data with a reasonable reliability and at a reasonable cost.

The maturity levels seen at the side of the figure, combined with four metrics aspects are used to demonstrate the influence of the maturity level on availability of data and cost factors.

To make it easier to read and interpret, the content of the figure is presented in the following table:

	1 Policy developed	**2 Procedures developed**	**3 Procedures and controls implemented**	**4 Procedures and controls tested**	**5 Procedures and controls integrated**
Metric types	Goals defined	Objectives Identified	Implementation	Effectiveness and efficiency	Impact
Collection automation	None	Low	Medium	High	Full
Collection difficulties	Very high	High	Medium	Medium to low	Low
Data availability	Non existent	Some data available	Can be collected	Available	In standard repository

We then apply this model to the Bank and assess the maturity of the security program, which the security metric will be a part of.

An assessment of the Bank by this model

The maturity level must be assessed on an average because it may vary within different parts of the organisation. It is certainly not static and will not automatically develop to a more mature state, because it is influenced by changes:

- In management - change in focus and support to security,
- Mergers and acquisitions – different business styles and maturity levels
- Business factors - e-business, “time to market” and increasing visibility of security to customers
- Technology with new security opportunities – i.e. MS Active directory with Kerberos and SAML [35]

A stabilising factor may be employees that have security knowledge and awareness. They will try to adjust their knowledge to the new business climate. This may slow down the impact of the changes.

The Bank developed a security program in 1994 starting with a policy, continued by procedures and a Baseline security requirements document. From the approval of the board in 1995, a series of compliance, risk evaluation and implementation campaigns have been run through several mergers and waves of change. The security framework has been revised several times during this 12-year period.

The IT operation was outsourced in 2001 and to have a reference point of the Bank’s own performance, the new vendor as a part of the agreement conducted a compliance survey. This showed an implementation rate estimated at approx 70% and the major deviations was addressed in a series of 5 improvement projects that was conducted in 2003 and 2004.

The Security analyses give a continuous campaign in making projects aware and comply with the framework and more than 400 analyses have been conducted since 1997.

There is a steady focus on testing security in electronic banking and e-business by system penetration, principles for secure code & code review [32] and IDS.

The security maturity is assessed as an average to be between level 3 and 4.

This leads to the following conclusions:

	3 Procedures and controls implemented	**4 Procedures and controls tested**	**Conclusions from applying the model to the Bank and the metric**
Metric types	Implementation	Effectiveness and efficiency	The metric is an **implementation metric** but will also be used to assess the effectiveness and efficiency of the security process, analysis, requirements and solutions
Collection automation	Medium	High	Collection automation is **low** as there is no IT support for the collection. Many of the answers from the questions in the Security analysis can be used as a basis for the measurement. Other data may be collected from the test-report, but they will – at this stage - be manually copied to the metric
Collection difficulties	Medium	Medium to low	The project organisation will have most of the data available, but it has to be collected from different sources and verified. **Medium difficulties.**
Data availability	Can be Collected	Available	The project organisation will have most of the data **available**, but to assess the data and to calculate a correct measurement will create some challenges

Focus should be given to automation of the data collection for the metric in order to reduce the workload and cost and to improve the reliability. (I.e. testing security instead of assessing security)

5.2.2 NIST 800-55 Metric detail form

The Metric detail form is designed to describe a metric for a specific performance indicator or security issue. Examples are given on how to measure *one security issue* like audit and logging across all systems in an organisation.

In our metric we will measure > 100 different security issues on *one single system*, and this form is therefore not directly applicable to this metric, but some concepts are very relevant and has been used in direct examples in the report.

The Metrics detail Form from 800-55		**Relevance to this metric**
Performance Goal	State the desired results of implementing one or several system security control objectives/techniques that are measured by the metric. When using NIST SP 800-26, this item will list a critical element, as stated in 800-26.	The desired result is related to each metric in a way described in the previous section
Performance Objective3	State the actions that are required to accomplish the performance goal. When using NIST SP 800-26, this item will list one or more subordinate questions, as stated in 800-26. Multiple performance objectives can correspond to a single performance goal.	The actions required – compliance - is related to each metric in a way described in the previous section
Metric	Define the metric by describing the quantitative measurement(s) provided by the metric. Use a numeric statement that begins with the words “percentage,” “number,” “frequency,” “average,” or other similar terms.	**The metric will use a number in a range from 0 – 4.** **See section on ISF metrics.**
Purpose	Describe the overall functionality obtained by collecting the metric. Include whether a metric will be used for internal performance measurement or external reporting, what insights are hoped to be gained from the metric, regulatory or legal reasons for collecting a specific metric if such exist, or other similar items.	The purpose – compliance measuring - is related to all aspects in the metric in a way described in the previous section
Implementation Evidence	List proof of the security controls’ existence that validates implementation. Implementation evidence is used to calculate the metric, as indirect indicators that validate that the activity is performed, and as causation factors that may point to the causes of unsatisfactory results for a specific metric. (Parenthesis in the original NIST document is removed due to space.)	**The idea is to strengthen the measurements' accuracy by listing several factors that point at degrees of implementation. This concept is important and will be used in the metric.**
Frequency	Propose time periods for collection of data that is used for measuring changes over time. Suggest time periods based on likely updates occurring in the control implementation. (Section 4.3, Feedback Within Metrics Development Process, contains a discussion on the frequency of metric data collection.)	The frequency – for all aspects in the metric - will be the same. The whole metric, or a subset, will be used at system delivery on demand.

The Metrics detail Form from 800-55		**Relevance to this metric**
Formula	Describe the calculation to be performed that results in a numeric expression of a metric. The information gathered through listing implementation evidence serves as an input into the formula for calculating the metric.	**The idea is that the formula is built on the Implementation evidence. This concept is important and will be used in the metric.**
Data Source	List the location of the data to be used in calculating the metric. Include databases, tracking tools, organizations, or specific roles within organizations that can provide required information. (Section 3.4.3, Data Management Concerns, contains a discussion on metrics data sources.)	**This concept is important and will be used in the metric, as it may increase reliability and reduce the workload of the metric.**
Indicators	Provide information about the meaning of the metric and its performance trend. Propose possible causes of trends identified through measurement and point at possible solutions to correct the observed shortcomings. State the performance target if it has been set for the metric and indicate what trends would be considered positive in relation to the performance target. (Section 4.2, Establishing Performance Targets, contains a discussion about the relationship of performance targets and the indicators.) Describe how the information gathered through listing implementation evidence is to be used as input into the analysis of indicators. The implementation evidence serves for validating performance of security activities and pinpointing causation factors	**The idea is to list possible causes of compliance failure identified through measurement and point at solutions both to correct compliance and the failure of the process.** **This area is of core interest to the Bank but will not be explored in this MSc report. It will be a part of the analysis of the measurements and the Bank will further develop the area later. Samples are given for illustration.**

The conclusion is to use the ideas that are **bold** as a part of the framework for the metric.

5.3 The principles in the ISF metrics

5.3.1 Information Security Forum (ISF)

The Information Security Forum is a member driven non-profit organisation, which delivers services like annual congress, security standards and metrics, workshops and issue reports on topics defined by members. ISF was established in 1989 and has grown to an international forum with 278 members with > 50% of the Fortune 500 included.

ISF has established the ”Standard Of Good Practice” SOGP [2] and the accompanying ”Information Security Status Survey”. The Survey is only available to members and measures compliance to SOGP and ISO 17799. In addition, it offers a benchmark comparison to the other members of ISF on the total or by business sector. The Survey consists of 5 types of questionnaires that cover different aspects like System Development or Critical Business Application.

ISF has also developed a simpler metric called “Security Health Check”.

ISF runs a project to develop a Meta standard that ties ISO 17799, ISF SOGP, CobiT and other standards together by a common structure and cross reference tables. The Survey, the Health Check and other metrics will be used to measure compliance against any of them.

What ISF does is quite similar to what the Bank wants and the principles of standards and metrics are presented in the following as input to a framework for the Bank’s metric.

To present this huge material in a useful way, content analysis has been conducted and the findings have been quality assured by interviews with the responsible managers in the ISF management team [33].

5.3.2 The Standard Of Good Practice - SOGP

SOGP is a comprehensive security standard from ISF available for free to the public. It has been developed and enhanced over a number of years, and is based on ISF members' “best practice”. Every 2 year, members are participating in workshops updating the standard with issues from real member experience, and the process has a greater flexibility and speed then the official standards bodies have.

SOGP has a way of relating different parts and nuances of the framework to responsible and contributing *aspects*. A security issue like Authentication may be covered from 5 different views by pinpointing which aspect each role is responsible for.

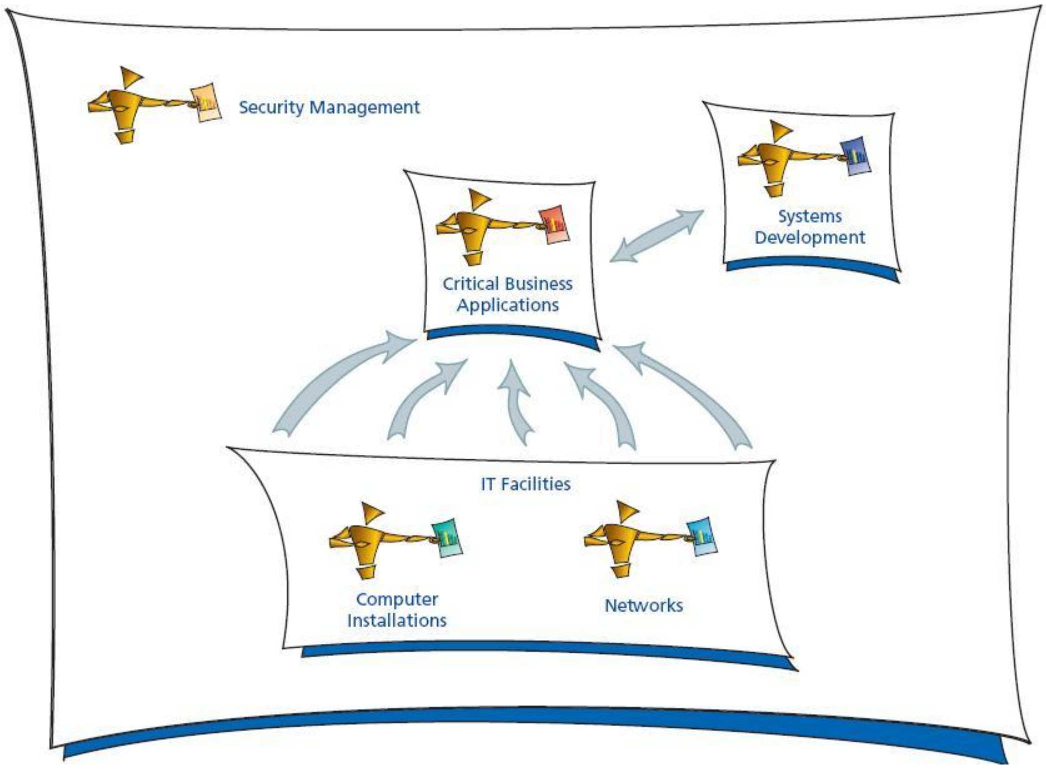


Figure 11 ISF: ASPECTS in SOGP

SOGP put business processes and therefore Critical Business applications at the centre of the model and relates the other activities to them as supporting activities. The security requirements relevant for each aspect are defined in separate sections in SOGP.

The Critical Business applications – CB - and the System Development – SD -sections are most relevant to the focus of this MSc thesis. CB focus on which security requirements are needed for critical systems while SD focus on requirements for a structured process when determining such requirements and when developing a system according to those requirements.

The standard has a unified structure: *Aspect, Area, Section, Control, Control detail.*

A closer look at the structure of each *aspect*:

- An introduction to the security *area* covered
- For each *section*:
  - A principle
  - An objective
  - A series of numbered security controls
    The numbering schema references aspect, section and control number
  - If there is more then one control detail in the sentence, each detail is labelled with a letter a, b...

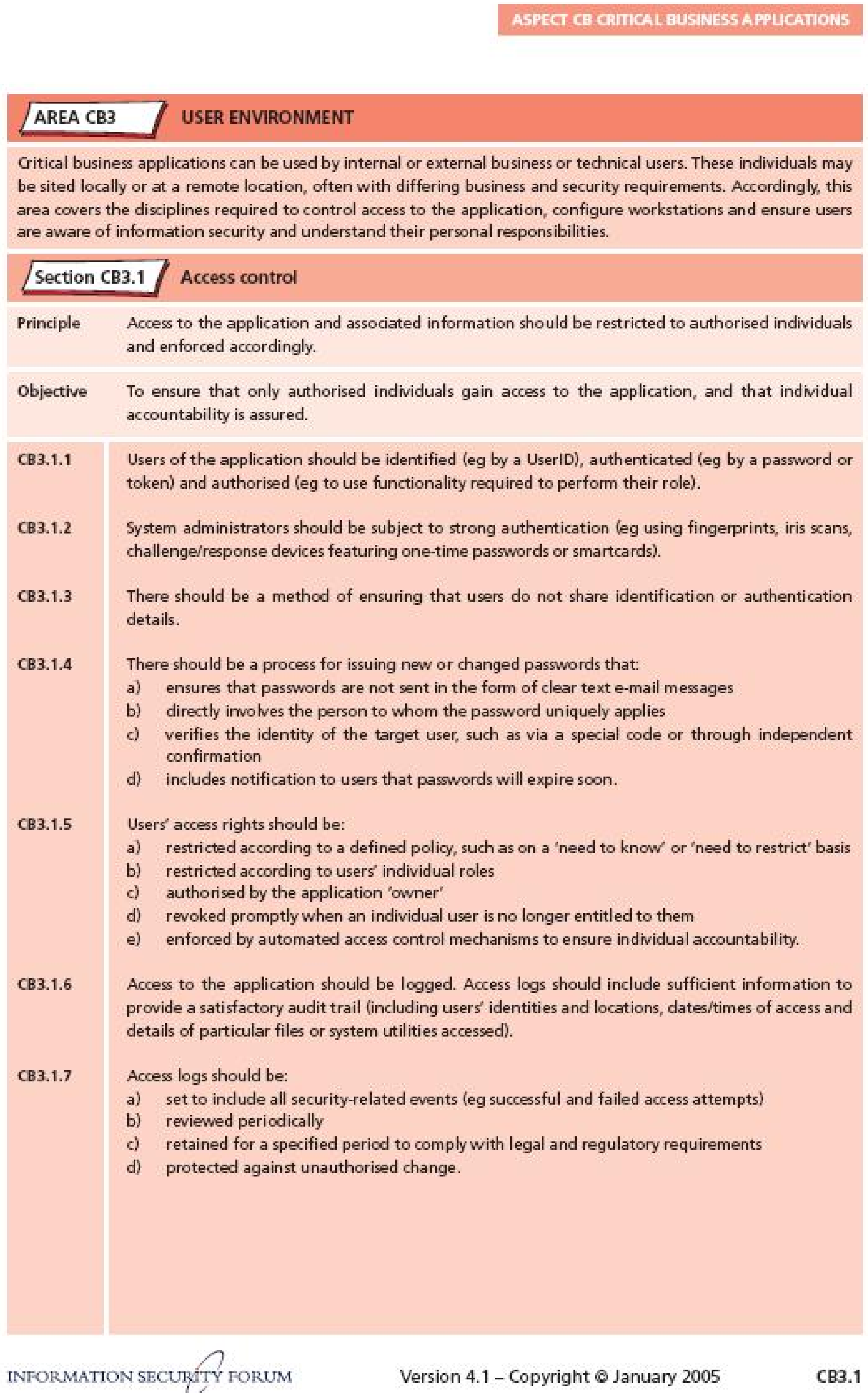
This structure makes it easy to find the control requirements for the aspect that the user need, and the numbering makes each detail addressable for compliance measurement.

An overview of the content of SOGP:

ASPECTS	**AREAS**	**SECTIONS**	**CONTROLS**	**Ctrl-DETAILS**
SM SEC. MGMNT	7	32	Ca 252	Ca 745
CB CRITICAL BUS.	6	25	121	348
CI COMP. INSTALL.	6	31	Ca 250	Ca 600
NW NETWORK	5	24	Ca 193	Ca 455
SD SYST DEVELOPM	6	23	Ca 143	Ca 399
TOT	30	135	Ca 1000	Ca 2500

Such a table does not exist in ISF's SOGP documents and the number of controls and control-details has been counted by hand in the CB aspect just for illustration. The estimates (Ca) are obtained from a real count based on the Survey, which is built on SOGP. A “guestimate” on the total of control-details (a, b, c...) in SOGP is around 2500.

An example from SOGP CB 3.1 is shown below in figure 12:



ASPECT CB CRITICAL BUSINESS APPLICATIONS

AREA CB3 USER ENVIRONMENT

Critical business applications can be used by internal or external business or technical users. These individuals may be sited locally or at a remote location, often with differing business and security requirements. Accordingly, this area covers the disciplines required to control access to the application, configure workstations and ensure users are aware of information security and understand their personal responsibilities.

Section CB3.1 Access control

Principle	Access to the application and associated information should be restricted to authorised individuals and enforced accordingly.
Objective	To ensure that only authorised individuals gain access to the application, and that individual accountability is assured.
CB3.1.1	Users of the application should be identified (eg by a UserID), authenticated (eg by a password or token) and authorised (eg to use functionality required to perform their role).
CB3.1.2	System administrators should be subject to strong authentication (eg using fingerprints, iris scans, challenge/response devices featuring one-time passwords or smartcards).
CB3.1.3	There should be a method of ensuring that users do not share identification or authentication details.
CB3.1.4	There should be a process for issuing new or changed passwords that: a) ensures that passwords are not sent in the form of clear text e-mail messages b) directly involves the person to whom the password uniquely applies c) verifies the identity of the target user, such as via a special code or through independent confirmation d) includes notification to users that passwords will expire soon.
CB3.1.5	Users' access rights should be: a) restricted according to a defined policy, such as on a 'need to know' or 'need to restrict' basis b) restricted according to users' individual roles c) authorised by the application 'owner' d) revoked promptly when an individual user is no longer entitled to them e) enforced by automated access control mechanisms to ensure individual accountability.
CB3.1.6	Access to the application should be logged. Access logs should include sufficient information to provide a satisfactory audit trail (including users' identities and locations, dates/times of access and details of particular files or system utilities accessed).
CB3.1.7	Access logs should be: a) set to include all security-related events (eg successful and failed access attempts) b) reviewed periodically c) retained for a specified period to comply with legal and regulatory requirements d) protected against unauthorised change.

INFORMATION SECURITY FORUM Version 4.1 – Copyright © January 2005 CB3.1

Figure 12 SOGP Sample

The reason for presenting the SOGP structure is that ISF metrics build on it and use of the structure is therefore relevant as input to the framework for our metric.

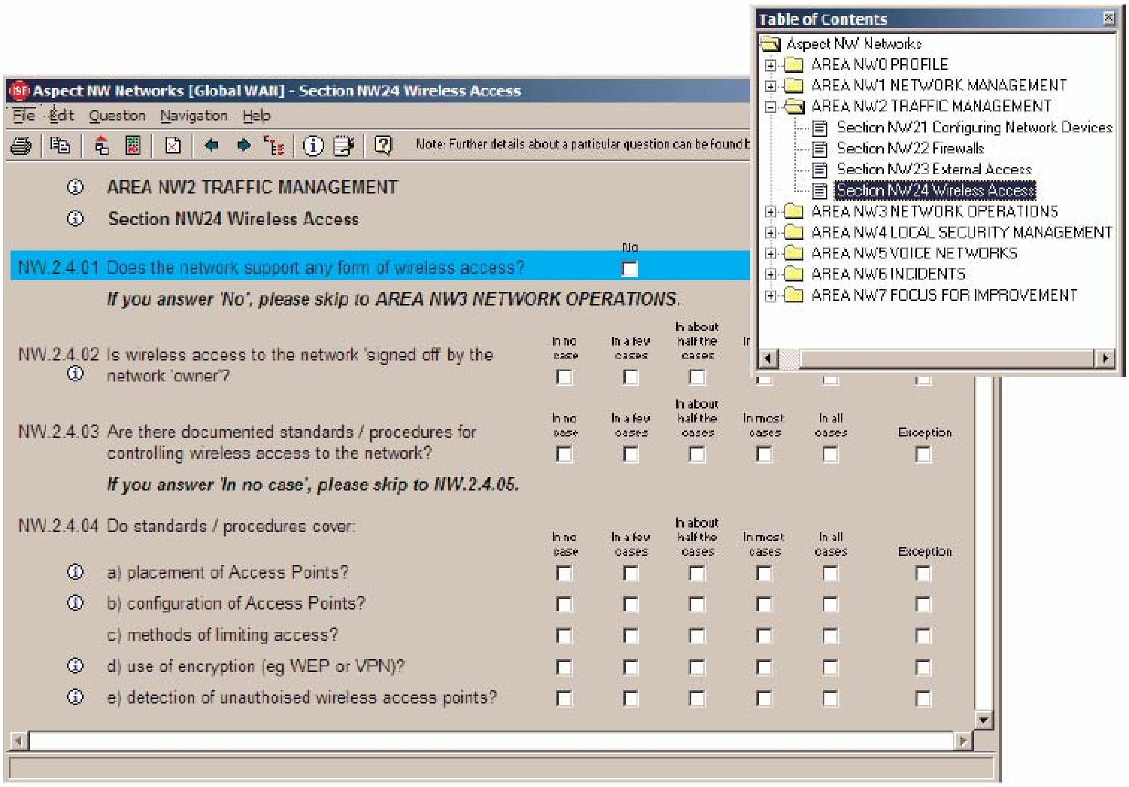
5.3.3 The survey

The Survey is a security metric to measure compliance to SOGP, and has therefore the same structure.

The "guestimate" on the total of control-details (a, b, c...) in SOGP from the previous section is 2500 and that the total number of questions in the Survey is at the same level, probing each control-detail with a question. For some details there is more than one question, which gives the total number of questions in the Survey of 2700+.

There is a questionnaire for each of the 5 aspects with an average of 500 questions where each question is related to a control detail in SOGP.

An example of a section from a Survey questionnaire


Aspect NW Networks [Global WAN] - Section NW24 Wireless Access
File
Edit
Question
Navigation
Help
Note: Further details about a particular question can be found b
Table of Contents
Aspect NW Networks
AREA NW0 PROFILE
AREA NW1 NETWORK MANAGEMENT
AREA NW2 TRAFFIC MANAGEMENT
Section NW21 Configuring Network Devices
Section NW22 Firewalls
Section NW23 External Access
Section NW24 Wireless Access
AREA NW3 NETWORK OPERATIONS
AREA NW4 LOCAL SECURITY MANAGEMENT
AREA NW5 VOICE NETWORKS
AREA NW6 INCIDENTS
AREA NW7 FOCUS FOR IMPROVEMENT

AREA NW2 TRAFFIC MANAGEMENT

Section NW24 Wireless Access

NW.2.4.01 Does the network support any form of wireless access? No □

If you answer 'No', please skip to AREA NW3 NETWORK OPERATIONS.

		In no case	In a few cases	In about half the cases	In most cases	In all cases	Exception
NW.2.4.02	Is wireless access to the network 'signed off' by the network 'owner'?	□	□	□	□	□	□
NW.2.4.03	Are there documented standards / procedures for controlling wireless access to the network?	□	□	□	□	□	□

If you answer 'In no case', please skip to NW.2.4.05.

NW.2.4.04 Do standards / procedures cover:

	In no case	In a few cases	In about half the cases	In most cases	In all cases	Exception
a) placement of Access Points?	□	□	□	□	□	□
b) configuration of Access Points?	□	□	□	□	□	□
c) methods of limiting access?	□	□	□	□	□	□
d) use of encryption (eg WEP or VPN)?	□	□	□	□	□	□
e) detection of unauthoised wireless access points?	□	□	□	□	□	□

Figure 13 Sample form in ISF Survey

As the Survey is testing at the detailed level of SOGP, it gives a fair overview of the compliance.

The survey is updated and run every 2 years as an ISF process. The ISF member can use the Survey as needed ranging from 1 questionnaire on any of the aspects to a set of questionnaires for each aspect. A typical set up for the Bank has been:

ASPECTS	**WHERE USED**
SM SEC MGMNT	2: 1 for the Bank group, and 1 for a subsidiary
CB CRIT BUS	5 critical business systems
CI COMP INST	5 operating systems/ platforms (Service provider)
NW NETWORK	1 network (Service provider)
SD SYST. DEV.	2 systems
TOT	**15 Questionnaires**

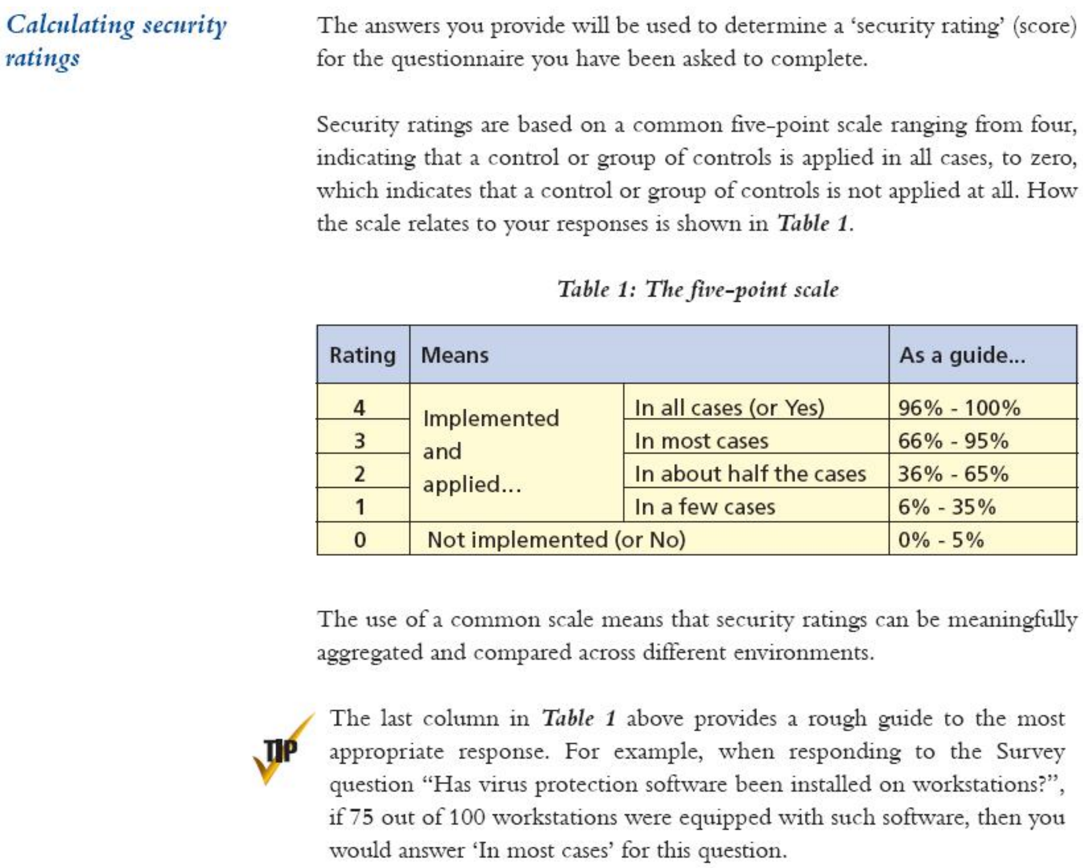
The member will have a comprehensive report back where the results are benchmarked against other members.

As there are more than 100 members participating in the Survey, ISF can issue an opinion on security matters on behalf of the members within reasonable confidence levels. The ISF survey is the only security metric to our knowledge that is regularly operated in this scale.

An obvious challenge with the SOGP and the Survey is the level of detail if you want to measure all aspects and with multiple questionnaires, one may enforce 15 x 500 = 7500 questions on the organisation and a substantial amount of work over a short period of time. Such a visible measuring project and investment creates expectations.

The Calculation of the security rating

The Survey uses the following formula and scale for calculating the rating or score:



Calculating security ratings

The answers you provide will be used to determine a 'security rating' (score) for the questionnaire you have been asked to complete.

Security ratings are based on a common five-point scale ranging from four, indicating that a control or group of controls is applied in all cases, to zero, which indicates that a control or group of controls is not applied at all. How the scale relates to your responses is shown in ***Table 1***.

Table 1: The five-point scale

Rating	Means		As a guide...
4	Implemented and applied...	In all cases (or Yes)	96% - 100%
3		In most cases	66% - 95%
2		In about half the cases	36% - 65%
1		In a few cases	6% - 35%
0	Not implemented (or No)		0% - 5%

The use of a common scale means that security ratings can be meaningfully aggregated and compared across different environments.

TIP The last column in ***Table 1*** above provides a rough guide to the most appropriate response. For example, when responding to the Survey question "Has virus protection software been installed on workstations?", if 75 out of 100 workstations were equipped with such software, then you would answer 'In most cases' for this question.

Figure 14 ISF: Calculating security ratings

This formula is used for all types of security questions and gives a consistent rating across the complete survey.

Reliability

A general problem with ISF metrics is that they are based on self-assessment, and there is no clear description of which "proof of implementation" is needed. The Survey imposes a workload due to several hundred questions, which may lead to quicker and less thorough assessments. This may lead to a systematic bias or random error that may cause reliability problems.

5.3.4 Security Health check

Because of the size and workload of the full Survey, members have asked for a "light" version and the result was introduced in 2005 in the form of Security health check.

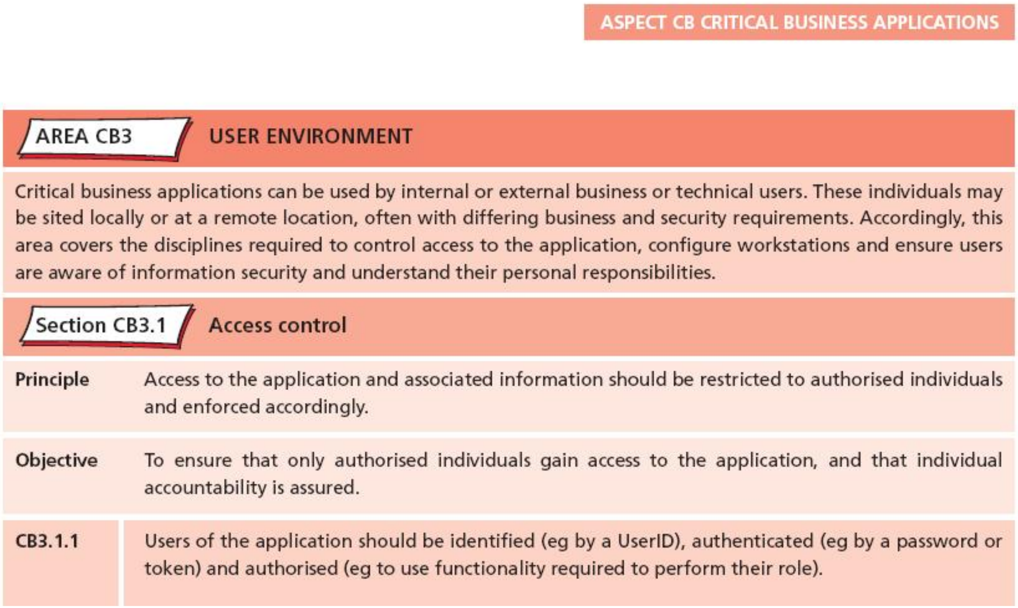
The Health check is still testing compliance to SOGP but on a much higher level as the total number of questions for all aspects, areas and sections is reduced from 2500+ to 170 questions.

Our analysis and interview showed that this reduction was done systematically by moving the Health check to test at a higher level in SOGP as illustrated in the following table:

ASPECTS	AREAS	SECTIONS	CONTROLS	Ctrl-DETAILS
SM SEC MGMNT	7	32	Ca 252	Ca 745
CB CRIT. BUS.	6	25	121	348
CI COMP INST	6	31	Ca 250	Ca 600

NW NETWORK	5	24	Ca 193	Ca 455
SD SYST DEV	6	23	Ca 143	Ca 399
TOT	30	135	Ca 1000	Ca 2500

As seen from this table, there are 135 sections and this is the level that Health check is testing on.



ASPECT CB CRITICAL BUSINESS APPLICATIONS

AREA CB3 USER ENVIRONMENT

Critical business applications can be used by internal or external business or technical users. These individuals may be sited locally or at a remote location, often with differing business and security requirements. Accordingly, this area covers the disciplines required to control access to the application, configure workstations and ensure users are aware of information security and understand their personal responsibilities.

Section CB3.1 Access control

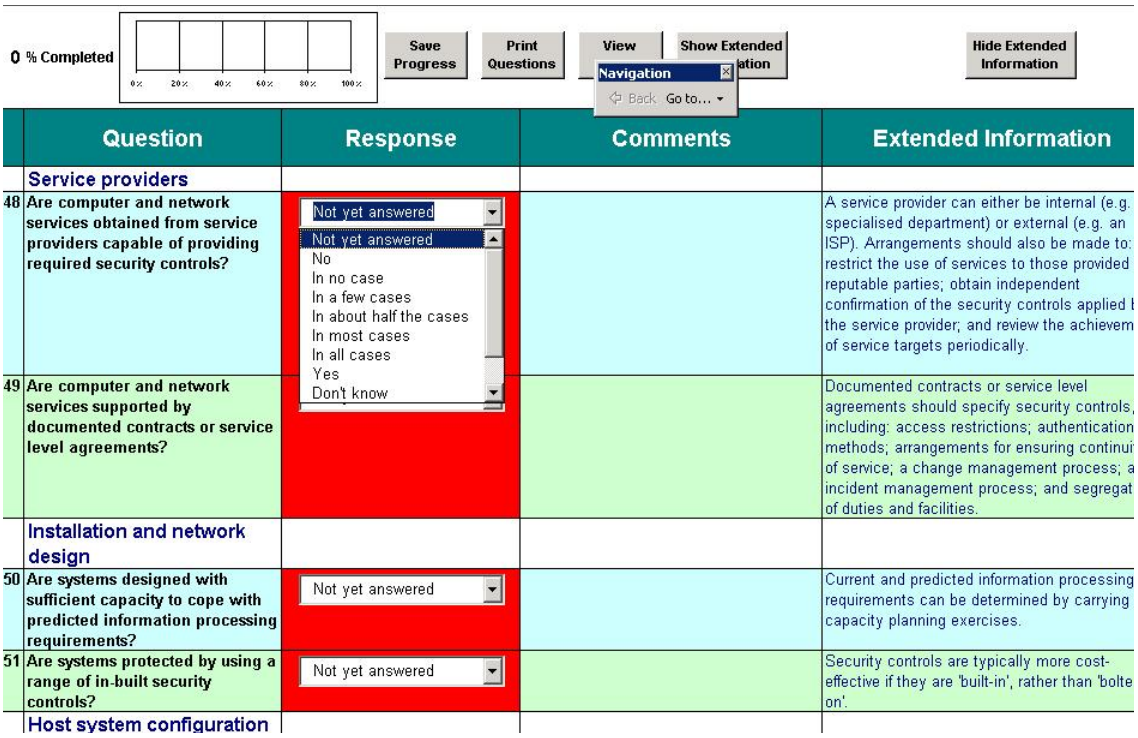
Principle	Access to the application and associated information should be restricted to authorised individuals and enforced accordingly.
Objective	To ensure that only authorised individuals gain access to the application, and that individual accountability is assured.
CB3.1.1	Users of the application should be identified (eg by a UserID), authenticated (eg by a password or token) and authorised (eg to use functionality required to perform their role).

Figure 15 Sample from ISF SOGP CB

Each section has the structure with Principle and Objective and by asking between 1 and 3 questions the sections principle and objective are tested for compliance by means of 170 questions.

It is obvious that by reducing the number of questions to < 10% of the original questions, the reliability may become an issue. It is therefore called checking and not measuring. The members is offered a tool to get an overview of –possible - weak areas in a large organisation and can then go deeper into these areas with the detailed Survey.

Sample from the Health check:



	Question	Response	Comments	Extended Information
	Service providers			
48	Are computer and network services obtained from service providers capable of providing required security controls?	Not yet answered		A service provider can either be internal (e.g. specialised department) or external (e.g. an ISP). Arrangements should also be made to: restrict the use of services to those provided reputable parties; obtain independent confirmation of the security controls applied t the service provider; and review the achievem of service targets periodically.
49	Are computer and network services supported by documented contracts or service level agreements?			Documented contracts or service level agreements should specify security controls, including: access restrictions; authentication methods; arrangements for ensuring continui of service; a change management process; a incident management process; and segregat of duties and facilities.
	Installation and network design			
50	Are systems designed with sufficient capacity to cope with predicted information processing requirements?	Not yet answered		Current and predicted information processing requirements can be determined by carrying capacity planning exercises.
51	Are systems protected by using a range of in-built security controls?	Not yet answered		Security controls are typically more cost-effective if they are 'built-in', rather than 'bolte on'.
	Host system configuration			

Figure 16 Sample from ISF Health Check

The layout of this metric seems suitable to use as a basis for the prototype metric in this project.

It is also an interesting and structured approach to reduce the level of detail in the metric – and the workload – by moving upwards to the Principle and Objective in each section. This can be used in this metric but the Bank's security documents do not have this clear-layered structure and we have to be careful when using such an approach.

5.3.5 Factors that reduces security incidents

As a part of the Survey, members also reports security incidents in a standardized form. By performing statistical analysis of the huge database of member surveys and incidents, ISF presented results several years ago that indicated that members with a high degree of compliance to *certain security controls*, had a significantly lower number and impact from Security incidents overall.

This was certainly of great interest to members and ISF presented a concept called "Bench mark factors" to highlight these controls or factors. The hope was that one could concentrate on a small set of security controls and gain a significant result in reducing the number and impact of incidents.

We therefore defined this as a topic in this assignment in order to use this to select the most important topics in the metric.

We interviewed relevant ISF management [33] on the matter. The result was not encouraging, as later statistical analysis did not confirm the first finding. Analysis in conjunction with the bi-annual Survey indicated relations between certain controls and low rate of incidents, but the actual controls varied with each bi-annually analysis and did not give stable indications on which controls.

Instead ISF management pointed out that certain factors – not controls – had a significant correlation with the number and impact of incidents. These factors are presented in ISF FIRM Special circumstances for a system or information recourse:

- Subject to a high degree of change
- Widely extended geographically
- Large in scale
- Complex
- Immature
- Accessible to external parties
- Used to support call centres

FIRM defines a spider graph to illustrate risk posed versus risk accepted.

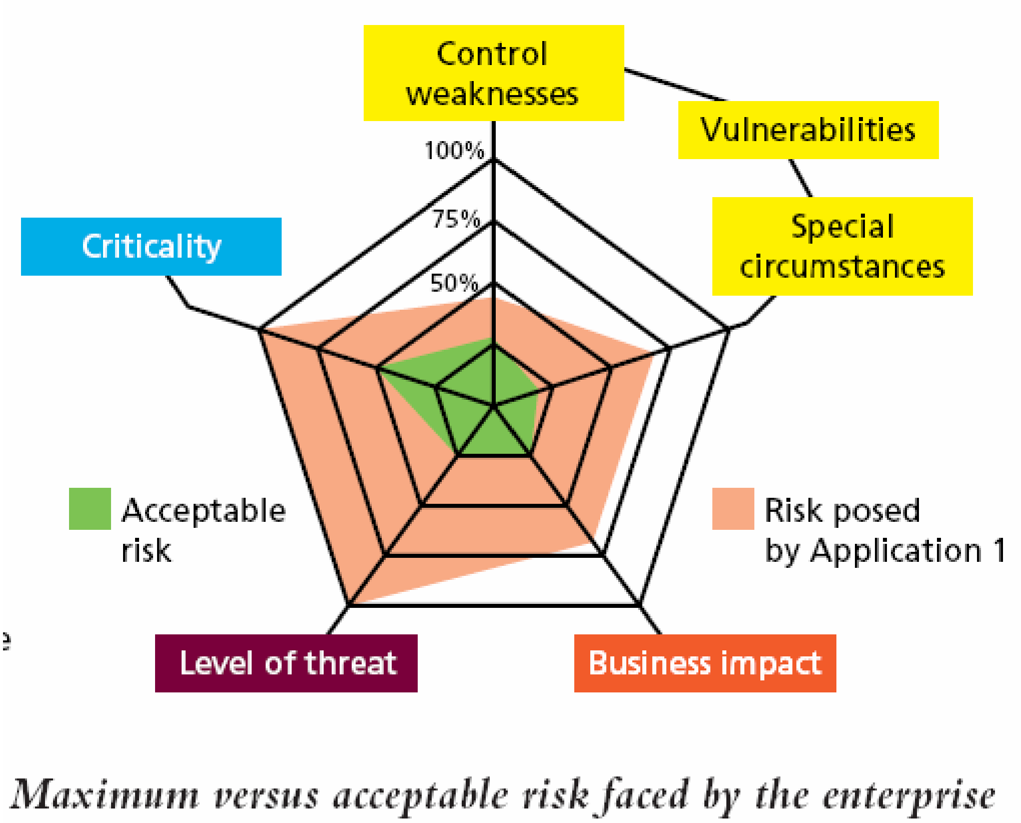


Figure 17 ISF: FIRM spider graph

This concept is rather complex and builds on a set of established methodology that one must follow to use it. FIRM is aimed at controlling risk in applications that are in production and on a high (not detailed) level.

The Bank has its own methodology aimed at system development, but the idea of expressing several risk factors in one picture may be used on a set of factors from the ”System Profile” section of the Security analysis and the following Security metric. Some relations can be seen between the ISF presentation and the – prototype – Bank risk factors.

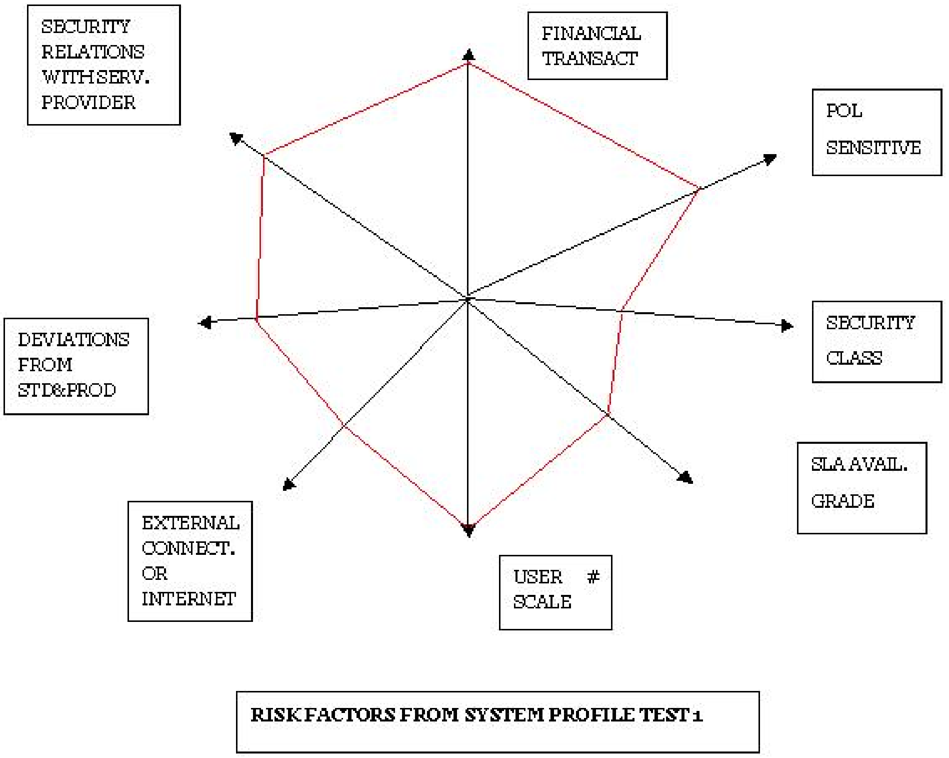

SECURITY RELATIONS WITH SERV. PROVIDER
FINANCIAL TRANSACT
POL SENSITIVE
SECURITY CLASS
SLA AVAIL. GRADE
USER # SCALE
EXTERNAL CONNECT. OR INTERNET
DEVIATIONS FROM STD&PROD
RISK FACTORS FROM SYSTEM PROFILE TEST 1

Figure 18 Risk factors from Test 1

The Right side of the Spider diagram presents important risk factors from a business point of view. By presenting them together, they may show inconsistence. The more spread they are, the greater the business need for compliance to security relevant for the factors.

RISK ASPECT	EXPLANATION	ADDITIONAL COMMENTS
Financial Transaction	If a system in the Bank can participate in Financial transactions, it has a risk of fraud.	The fraud could be false transactions, false beneficiaries etc depending on the setting. If the service is unlimited and includes payments abroad, the risk of loss increases.
POL [36] sensitive	The Norwegian Privacy act – POL – defines certain info as Sensitive which requires stronger security measures	FPOL [37] defines stronger requirements for systems that handle Sensitive information, i.e. medical status or sexual orientation. A typical example from the Bank group would

RISK ASPECT	EXPLANATION	ADDITIONAL COMMENTS
	regarding confidentiality	be medical status in appliance for life insurance which is defined Sensitive by POL [36].
Security class	The Security analysis requires the system to be risk analysed and classified with respect to Confidentiality Integrity Availability	13 Class: Red/High, Blue/Medium, Yellow/Low, or isolated? (Builds on Risk Analysis forms for C, I, A 0 Little damage 1 Some damage 2 Substantial damage 3 Very serious damage 4 Business at risk).

SLA availability grade	The SLA Availability grade for the system indicates the business importance of availability and increase in risk	SLA Availability grade
		A= 99,7 within "opening hour" 24/7
		B= 99,7 within "opening hour" 08-22
		C= 99,7 within "opening hour" 08-17
		The difference between A and C is more than 7400 service hours pr year or a factor of 3.7 which gives a totally different challenge to the organisation, the resilience and maintenance of the system

User # scale	User # scale indicates if the system is used by a small or large number of users	If the number of users is large, the total business impact of non-compliance increases. I.e.: non-standard authentication, lack of SSO, extra password problems and lack of role based and business oriented access administration.

The Left side of the Spider diagram presents important risk factors from a technical point of view. By presenting them together with the business point of view, they may indicate a threat level that needs special attention and stronger security controls.

RISK ASPECT	EXPLANATION	RELEVANCE / COMMENTS HERE
External connections or Internet	The potential risk increases if the system has external connections, has external users and even more so if the system is exposed to the Internet.	The Bank has created a secure infrastructure for Extranets, Internet banking and e-commerce with IDS and regular system penetration. If the system has deviations from this infrastructure, Service provider or from Standards and products, the needed security level may be a challenge to achieve.
Deviations from Standards and products	The potential risk increases if a system is built on "new" or non-standard technology that has never been security analysed before. This also	The advantage of scale is eroded and the challenge for all involved parties increases to be assured that *facts* are known and a secure mature solution is found. The recourses and skills to do this properly may not be available.

RISK ASPECT	EXPLANATION	RELEVANCE / COMMENTS HERE
	often excludes the recommended security solutions as they may not be supported in the special environment.	
Security Relations with the Service Provider	The potential risk increases if the SP is "New", is unfamiliar with the Bank's Security Requirements and the contractual security obligations are weak.	A standard security appendix is now required for contracts with external SP and lays the ground for a structured and measured relation with the SP, but this appendix may not be a part of the contract.

The prototype shown is used to illustrate the concept of a complex risk diagram, but will not be defined in detail in this MSc thesis, and will be listed for further work.

5.4 A summary of the chosen framework

At this stage we have a framework for the metric:

We have used the three-step method to define performance topics, critical success factors and performance indicators for each success factor:

- The main purpose of the metric is to manage risk associated with loss of Confidentiality, Integrity and Availability
- The performance indicators for each success factor for this metric are the compliance to the security requirements and the security process. (Areas of non-compliance indicate lack of success).
- Analysis of the areas of non-compliance, the associated risk and the root cause will be important parts of the risk management

We have described and analysed the Stakeholders – the users of the metric:

STAKEHOLDER	REASON
Project manager / Business developer	To document security status and learn from their own performance.
System owner / Business owner	To know the security status when they take over the responsibility from development.
Top management	To manage risk and to quality assure facts before they report externally to reduce their personal liability.
Management of System development	To collect statistics to see trends of systematic problems and flaws in development processes that lead to security problems.
Head of IT Security	To assist top management in managing risk and to manage and the security process and deliverables (i.e. Security analyses).

We have demonstrated the importance of Clear line of sight and accountability:

- By measuring within the scope of a development project
- By selecting the requirements in BSR that are relevant to System development

We are aware of the effect of measuring – "You become what you measure" and will take this into account in the next chapter in selecting the content of the metric.

We have assessed the Security program maturity of the bank to between level 3 and 4 and concluded that there will be medium difficulties in collecting data for measurement. Focus should be given to automation of data collection to increase the reliability and reduce the workload of the metric. If the collection can be combined with testing security implementation, the program maturity increases.

We will use NIST concepts of:

- Implementation evidence to increase the reliability by listing factors or ask questions that indicate the degree of compliance.
- Source to describe the most reliable and accessible source for measurement data

We will use the concept of ISF SOGP and metrics to measure at the optimal level of detail and will use the layout and measurement scale of the Security Health check.

We will present selected risk factors from the System profile section of the measured system in a Spider diagram. This may assist the user in focusing on the most important non-compliance areas and associated risk.

6 Defining the content of the metric

The next step was to carry out a qualitative Content analysis of the 60 questions of the Security analysis and to compare them with the 200 Baseline Security Requirements to establish an overview of the security topics covered. To do this we need an overview of the problem and research question again.

It was defined like this:

"The research question is how to define a security metric that measures the security status of a new system at delivery in an objective and concise manner.

The term *security status* can be defined from different points of view:

- The degree of compliance to the advice of solutions and requirements included in the Security analysis of the system
- The degree of compliance to (a subset of) the Bank's BSR
- To explain the security status and area of non-compliance in terms of the business need for Confidentiality, Integrity and Availability

The scope of the *security status* must be decided in the thesis from a reasonable combination of these points of view."

The analysis of the related documents was performed in steps in order to assure that the chosen metric could be traced back to each component of this reasonable combination:

- To analyse the "advice of solutions and requirements included in the Security analysis" and present the content in a form suitable for analysis and cross reference to the Bank's BSR
- To analyse the Bank's BSR, define the subset of requirements relevant to system development projects and to cross reference the content of the Security analysis to these requirements

  This would clarify some important facts:
  - Which subset of security requirements from BSR were the projects obliged to comply to?
  - Do the solutions and requirements in the Security analysis cover these requirements in a reasonable way?
  - Does the Security analysis present any solutions or requirements that are not rooted on the Bank's BSR?
- To analyse the relevant ISF metrics and cross reference with relevant parts to the Bank's BSR

6.1 Background on the Bank's security approach

To understand the Security analysis and the Security Metric, one must understand the approach that the Bank takes regarding security in system development.

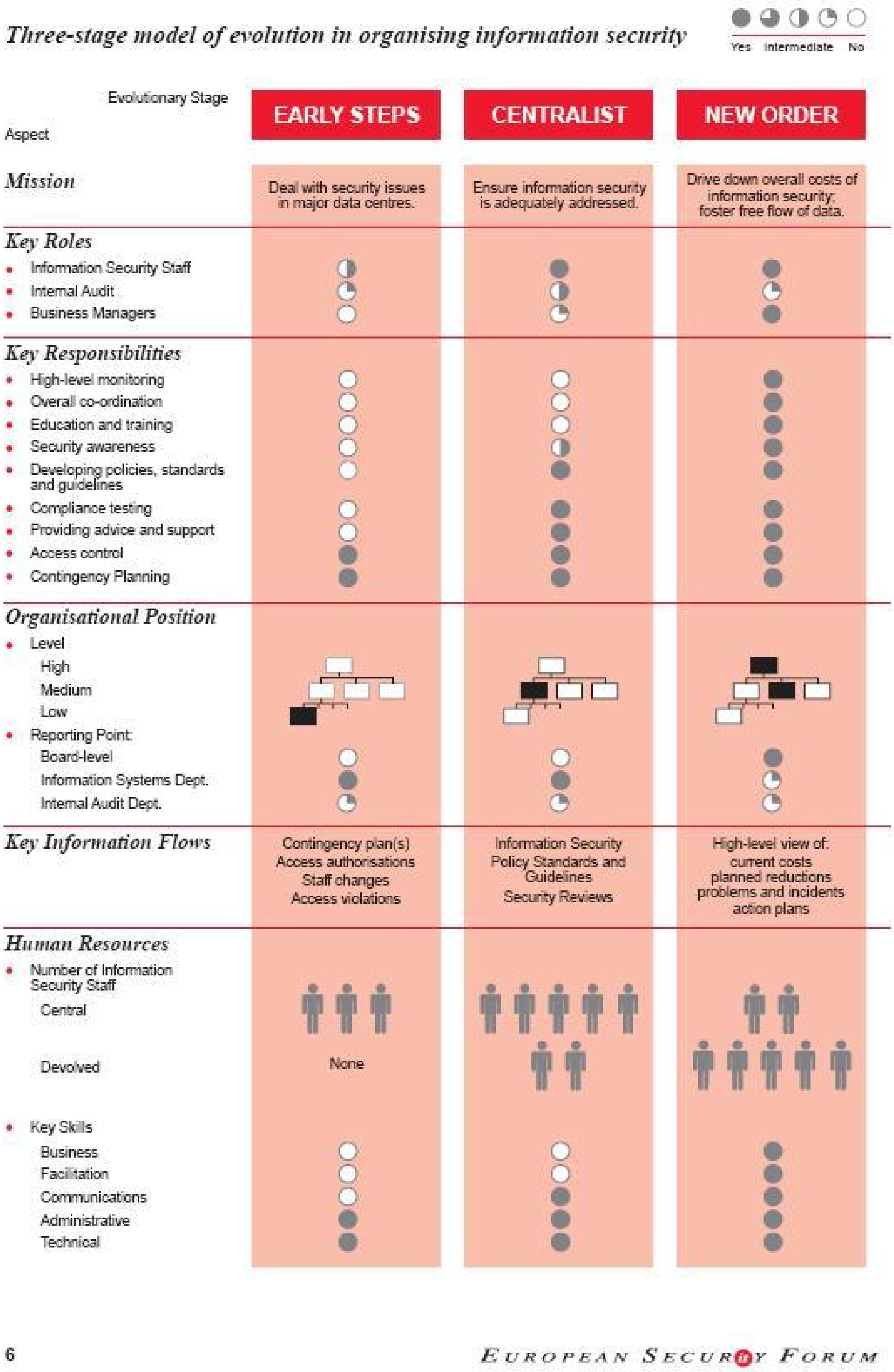
Security frameworks like SOGP and ISO 17799 define security requirements that focus on the security context of each system as if they were isolated. They have lesser focus on how these requirements can be defined and interpreted to achieve:

- Ease of use – user perspective
  - Single sign-on or more realistically: reduced burden of sign-on
- Ease of administration – management perspective

  - Effective process, Single point of administration, role based and business focused
- An advantage of scale in the security field – Business and IT perspective
  - Security architecture, standards, reusable solutions and processes

Because these issues are not clearly defined or understood in the security standard, many businesses implement security by a "tunnel vision" that – isolated – seems to cover the security requirements but may lead to:

- Heavy burden for the user
  Many UserIDs, passwords and different sign on leads to user problems and low security image and motivation
- Slow and in-transparent service for managers and business
  Many administration processes, tools, technical access details lead to low service performance in providing correct access, fragmented reporting on access and removal of access.
- Slow and costly IT-development and operation
  High complexity, lack of standards, spread of skill on many solutions lead to high operational risk and cost, variable security level, and slow delivery



Three-stage model of evolution in organising information security

● ◕ ◑ ◔ ○
Yes Intermediate No

Evolutionary Stage Aspect	EARLY STEPS	CENTRALIST	NEW ORDER
Mission	Deal with security issues in major data centres.	Ensure information security is adequately addressed.	Drive down overall costs of information security; foster free flow of data.
Key Roles			
• Information Security Staff	◑	●	●
• Internal Audit	◔	◑	◔
• Business Managers	○	◔	●
Key Responsibilities			
• High-level monitoring	○	○	●
• Overall co-ordination	○	○	●
• Education and training	○	○	●
• Security awareness	○	◑	●
• Developing policies, standards and guidelines	○	●	●
• Compliance testing	○	●	●
• Providing advice and support	○	●	●
• Access control	●	●	●
• Contingency Planning	●	●	●
Organisational Position			
• Level			
High			
Medium			
Low			
• Reporting Point:			
Board-level	○	○	●
Information Systems Dept.	●	●	◔
Internal Audit Dept.	◔	◔	◔
Key Information Flows	Contingency plan(s) Access authorisations Staff changes Access violations	Information Security Policy Standards and Guidelines Security Reviews	High-level view of: current costs planned reductions problems and incidents action plans
Human Resources			
• Number of Information Security Staff			
Central	👤👤👤	👤👤👤👤👤	👤👤
Devolved	None	👤👤	👤👤👤👤👤
• Key Skills			
Business	○	○	●
Facilitation	○	○	●
Communications	○	●	●
Administrative	●	●	●
Technical	●	●	●

6 EUROPEAN SECURITY FORUM

Figure 19 ISF: Three stage model of evolution

ISF pointed this out very early in the report "Organizing security for the 90's" [38]

In the right column "New order" the following can be observed:

The mission (first row) has changed from "Ensure information security is adequately addressed" to "Drive down overall cost of information security and foster free flow of information". The main reason for this shift is that if the earlier evolutionary stages succeeded by increasing awareness and knowledge of security issues and requirements, then the business users will see the result as security "popping up" everywhere and the burden of unstructured security arrangements becomes evident.

The Bank defined the Baseline Security Requirements in 1995 and saw gradually the shift from discussing "what" to "how" these security requirements should be solved in a business oriented way.

Long term security goals were defined in order to support business focused security: reduced sign on, more efficient administration based on business roles and better reports to increase awareness on authorized access. At the same time the central Security department started developing security architecture and buying or building solutions to support it.

The new challenge for the Security department was to convey this security concept to development projects in a form understandable to them. The Security analysis was developed to assist this process and to quality assure that different security consultants addressed the same issues and gave the same recommendation on the security concepts.

6.1.1 Challenges related to the Bank's documents and analyses performed

The content analysis that has been performed on the Security analysis involved a translation of the main content without having to make a complete English version first. To assure that the translated content analysis is a fair representation of the original, the numbering of sections and questions in the original is kept in the content analysis, and transferred to the resulting metric. To ensure the correct interpretation of a metric, one can always look up in the original.

The Bank is doing a major update on the security requirements document due to the merger of two large banks and at the same time the basic structure of the document is changed to an ISO 17799 style.

As a basic function of the security analysis is to assist compliance to the security requirements, this update also creates a need to update the Security analysis.

This situation was debated with the Bank's reference group and the conclusion was:

- The Bank does not need an English version of the metric at this stage,
  a Norwegian version is needed first
- The content of the Security analysis and metric will have to be updated by the Bank due to changes in the Bank's IT security documents
- Focus in this assignment should therefore be kept on ideas on what and how to measure in a prototype in stead of a complete English metric with correct sentences and final form

6.2 The Security analysis

The Security analysis is a (Norwegian) word template document. The project manager uses the development process in the quality system and the Security analysis is one of the required documents to get a system development project approved. This is to ensure that security challenges, requirements and recommended solutions are known to the project before detailed plans and cost estimates are made.

The Security analysis consists of 4 main sections:

1. Introduction
    a. To understand the analysis and the associated process
    b. Security roles and responsibility for the project
2. System profile
    a. To understand the business needs, importance, perspective and legal limits
    b. System drawings, project scope, type of project and system, integration
    c. A simple risk analysis and a concluding security classification
3. Control selection
    a. To select adequate security solutions for the project's business functions depending on topics like internal or external users, secure payment instructions, level of contingency etc
    b. The security topics and controls covered in this section:
    Authentication & Identity management, Access control & role based access management, Password process, Access control for programs, Securing application data, Network & data exchange, Secure code & penetration testing, Audit, logs & incident management, Resilience & contingency, Technical Platform & infrastructure, System maintenance & Operation, Agreements (SLA, 3.party)
4. Risk summary
    a. A concluding list of areas of possible non compliance, uncovered risk and possible consequences
    b. Planned countermeasures to mitigate risk

The content analysis summary in security key words can be seen in appendix A.

Samples of the content are presented in the following to explain the Security analysis modus operandi. The Security metric is based on the same structure

6.2.1 The control selection by Application type

The control selection is presented here because it is a special construction and is essential to use the analysis correctly. It demonstrates the diversity of environments and security challenges that the Bank faces in the age of e-commerce, partnership and providing IT service to externals.

As the structure of the metric follows the Security analysis, the Control selection is repeated in the metric.

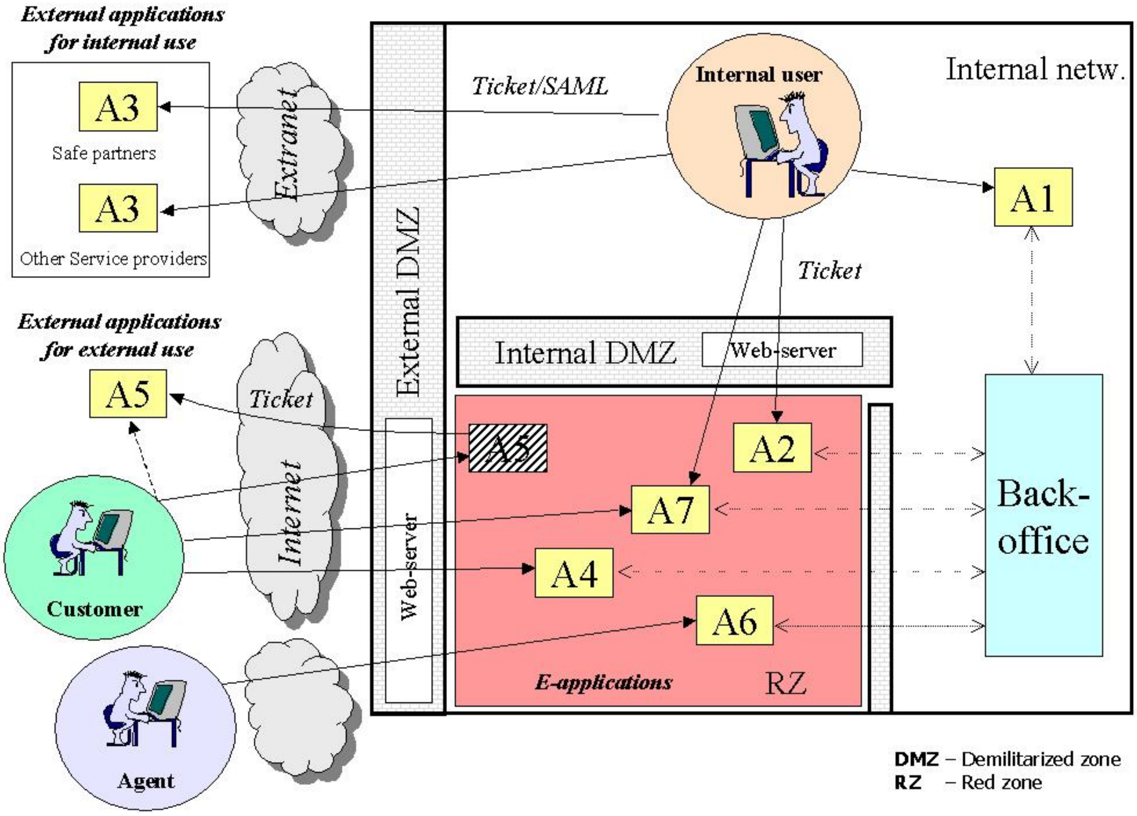


Figure 20 Application types

A1: Internal application for internal users	□	Chap 5.2.2
A2: E- application for internal users	□	Chap 5.2.2
A3: External application for internal users	□	Chap 5.2.4
A4: E- application for customers	□	Chap 5.2.3
A5: External application for customers	□	Chap 5.2.3
A6: E- application for agents	□	Chap 5.2.3
A7: Common E-application for both internal users and customers	□	Chap 5.2.2 & 5.2.3
Other (specify):		Chap 5.2.2 – 5.2.4

By studying the figure above and ticking off the relevant sections, the project can jump to the relevant chapters of the Security analysis and ignore the rest. Each chapter has tailored the recommended security solutions to the application type – if the Bank has a relevant solution.

Each chapter and security topic has the following general structure:

Y.yyy Security topic (i.e. sign on)

ⓜ Information or recommendation given to the project.
Example:
Single Sign-On reduces the burden of logon for users and can be achieved by utilizing the Kerberos function of Active Directory in W2000.
See ”SSO.doc” for a description of the standardized Kerberos service in the Bank, which also includes a function for generating an ACF2 ticket to the host.

Q x Will the users be required to log on separately to the system (or will SSO be used)

No □ ⇩ Please describe how SSO is achieved:

Yes □ ⇩ Please answer the following additional questions:

1. What technical platforms and databases must the user log on to?
2. Is an attempt made with the vendor to eliminate or simplify the logon?
3. Have the consequences of an extra logon been evaluated?
4. Describe any deviation from UID standard.
5. Describe any deviation from Password requirements ref. BSR chap 5.1.2.1.1.
6. Describe how UIDs and passwords are stored securely in this solution.
7. Describe how security audit/logging is covered, ref. BSR chap. 6.5.1.1.1 og 6.5.1.1.2.
8. Which tool and process is used to administer users, access and passwords?

The elements work together in the following way:

- The chapter nr Y.yyy with heading states the security topic (the example here is Sign on and authentication)
- The M-box with colour gives information on which security solution (here SSO) we recommend in the context of an application type (here Internal application for internal user as ticked off in the table on the previous page)
- The Question Qx (x is the question number) asks the project whether they do not follow the recommendation or if they do
  (here the question is “negative” - it asks if user have to do a separate log on).
- No - in this case - means that the recommendation for SSO is followed an the project describes how this is solved
- Yes - in this case - means that the system will impose an extra Sign on to the user and the analysis has to check that the burden and total consequences of “yet another sign-on” is known and accepted by the business owner and that the chosen solution is secure according to the Bank’s requirements and existing processes for UserID, Passwords, logging and administration

The more deviations from the Bank's standards and common processes each step reveals, the heavier the burden for the business user or less secure solution. In an organisation with more than 10.000 users and > 500 business applications, standardisation leads to advantage of scale and the opposite leads to fragmented security.

6.3 The content analysis of the Security analysis

The content of the Security analysis was analysed and presented in a table as demonstrated below. For comparison, the same elements of the Security analysis presented in the previous section are presented in a tabular form here.

CH #	SECTION & PURPOSE	INFO GIVEN TO PROJECT	QUESTIONS TO AND ANSWERS FROM PROJECT	BSR ref
5.2	**Access control selection** Type of users and application to jump to relevant section in SA	Table: - type of user, # of each type - in which part of the system	17 Type of user: Internal, SystemAdm, Superuser, Customer care/adm, Eksternal user/customer, Agents, Admin at external site	
	Select one or two-factor authentication, reduced sign on, avoid external exposure of internal functions	Illustration fig. Table: - type of application environment	18 Type of application environment: Internal appl. for internal users, Web for internal, Web for external, External appl. for internal, Web for customers, Web for Agents, Common web application for internal & customer, other type	
5.2.2	Internal appl. For internal users			
5221	Authentication and Identity mgmnt	UserID std Single Sign-On Password reset process Password harmonisation	19 User IT platform (W2K or ACF2) 20 Extra log on, YES=> 10 additional questions Describe logon, eliminate?, consequences evaluated, UID std & PW requirements deviation, PW storage secure, security logging, admin tool and process, PW reset	5.1 5.2 5.4 6 6.5

5222	Authorisation, Access control, Access mgmnt	Preferred sec. systems Design model Avoid internal tables Sec.Adm.Mgr SAM Business Access roles Admin process Describe in standard formulary Internal access to e-applications via internal DMZ (not external)	21 Internal solutions/tables 22 Describe access solution 23 use of SAM and Business access roles 24 Avoid external exposure of internal functions	5.3 5.4

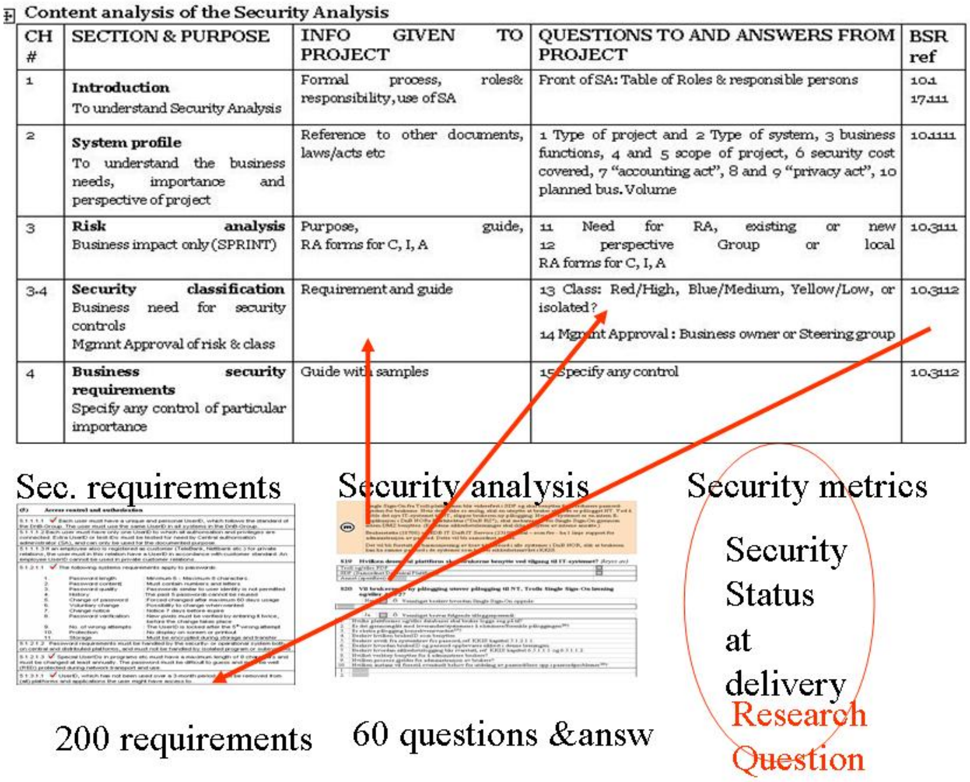
To give a useful representation of the content of the full Norwegian document in English, only the key words of the security content have been used. This would indicate the topics to be measured in the Security metric.

An explanation of the columns in the table starting from the left:

- The 1. and the 2. column gives the structure of the document by the section number, section heading and the purpose of the section
- The 3. column "INFO GIVEN TO PROJECT " lists the information given in the analysis to the project regarding how to use the analysis and which security solution that is preferred on the subject being analysed.
- The 4. column "QUESTIONS TO AND ANSWERS FROM PROJECT" list the security keywords of the questions that the project will answer in the analysis
- The 5. column cross refer to the section in the Bank's BSR to demonstrate that the topics covered in the Security analysis are rooted on defined requirements

The 3. and 4. column contain the basic topics that the metric must cover to fulfil the assignment.

The 5. column demonstrates that the topics covered in the Security analysis – as a whole -are rooted on the Bank's BSR. The detailed findings of this part of the analysis are not relevant for the research question, but will be given in the section 8.4 *Findings - not related to the research question*.



Content analysis of the Security Analysis

CH #	SECTION & PURPOSE	INFO GIVEN TO PROJECT	QUESTIONS TO AND ANSWERS FROM PROJECT	BSR ref
1	**Introduction** To understand Security Analysis	Formal process, roles& responsibility, use of SA	Front of SA: Table of Roles & responsible persons	10.1 17.111
2	**System profile** To understand the business needs, importance and perspective of project	Reference to other documents, laws/acts etc	1 Type of project and 2 Type of system, 3 business functions, 4 and 5 scope of project, 6 security cost covered, 7 "accounting act", 8 and 9 "privacy act", 10 planned bus. Volume	10.1111
3	**Risk analysis** Business impact only (SPRINT)	Purpose, guide, RA forms for C, I, A	11 Need for RA, existing or new 12 perspective Group or local RA forms for C, I, A	10.3111
3.4	**Security classification** Business need for security controls Mgmnt Approval of risk & class	Requirement and guide	13 Class: Red/High, Blue/Medium, Yellow/Low, or isolated ? 14 Mgmnt Approval : Business owner or Steering group	10.3112
4	**Business security requirements** Specify any control of particular importance	Guide with samples	15 Specify any control	10.3112

Figure 21 Content analysis of the Security analysis

6.4 The content analysis of the Bank's security requirements (BSR)

The next task was to analyse the Bank's BSR, define the subset of requirements relevant to system development projects and to cross reference the content of the Security analysis to these requirements.

The Bank's BSR is a word document that also exists in an English version, so here a translation was not necessary.

The first step was to define the subset of requirements relevant to system development projects. The BSR defines a set of security requirements for typical roles of an organisation:

- Business roles
  - End user
  - Business manager
- IT-roles
  - System owner or project manager
  - IT Operational and system technical
- Security roles
  - Security department

The document has an appendix with the approx. 200 security requirements in a tabular form. Each requirement is attached to a role that is the principally responsible to fulfil that requirement, but also indicate which roles are expected to contribute to fulfilling the requirement.

This requirement & responsibility matrix has been modified as a basis for this analysis as it already gave a definition of what each role was responsible for.

The requirements attached to the System owner or project manager constituted a reasonable starting point. All requirements were walked through again to se if there were other requirements that the projects also should support even though another role had the main responsibility for them.

As a result all requirements regarded as not relevant to system development projects were marked with a grey tone.

4.1.2.1.1 Employees must be trained in correct use of data systems, as well as relevant parts of the Baseline Security Requirements in connection with their assigned privileges.
4.1.3.1.1 ✓ Manager must ensure that all employees assigned roles are familiar with tasks, responsibility and authority

In this example only the first requirement is regarded as relevant for a development project, because a project in the Bank is supposed to contribute with relevant training for the user as a part of delivery and roll out. The second requirement is the business manager responsibility and the assignment of business people to roles and the according responsibility is not a reasonable part of a project scope.

6.5 External validity: ISF's Standard of good practice - SOGP

ISF's Standard of good practice - SOGP - supports this way of relating different parts of the framework to responsible and contributing aspects or roles.

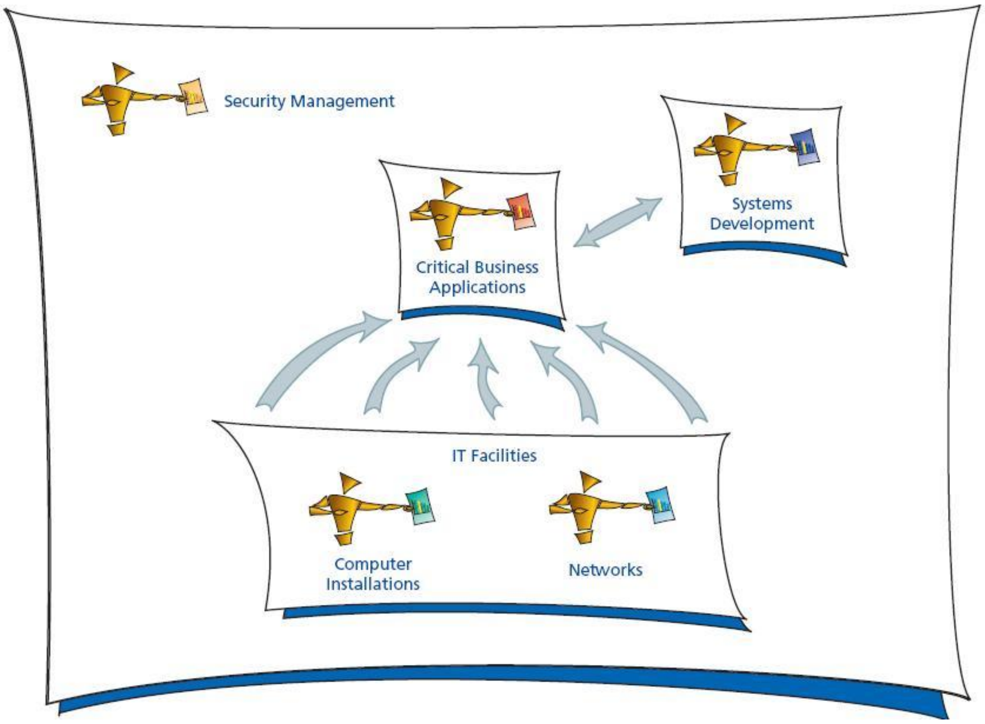


Figure 22 ISF: ASPECTS in SOGP

SOGP defines the business processes and Business critical applications as the centre of the model and regard the other processes as supporting activities to that business focus. The security requirements relevant for each aspect are defined in a separate section in SOGP as described in section: *The standard of good practice*

The Critical Business application CB and the System development SD sections are relevant to the focus of this MSc thesis. Due to time constraint in this assignment only CB has been used as a standard to improve the external validity of the metric. The analysis was conducted by cross-referencing BSR requirements with the SOGP CB requirements to evaluate:

- If the SOGP requirement was reasonably covered in BSR
- If SOGP has requirements in excess of BSR that are relevant to the Bank and the research question and therefore should be included
- If requirements in BSR were not covered in SOGP, were relevant to a general standard and therefore should be proposed as a member improvement proposal of SOGP to ISF

The notation in the cross reference to SOGP can be illustrated by examples::

REQUIREMENT	REF.
6.2.4.1.1 The component/system that produces logs must have a synchronised date and clock for all systems in the Bank. Maximum 2 seconds between actual time and "system-time" should be allowed.	SOGP IMPROVE
6.3.1.1.1 ✓ The System Owner shall determine what kind of business information needs to be logged, and must ascertain a consecutive and understandable chain of evidence, which can document who is responsible if there are cases of complaints, errors or fraud.	CB 2.2.6
6.3.1.1.2 In the systems where customer transactions involve several sub processes and various technical systems before accounting, at least 2 independent log points are required.	
CB 6.1 Third Party agreement CB6.1.1 Third parties that require access to the application (i.e. external organisations, such as customers or suppliers and members of the public) should be subject to additional controls.	

The first *row* represents a BSR requirement that is not covered in SOGP, but is relevant to a general standard and therefore should be proposed as a member improvement proposal to ISF. In fact this and other findings have this spring been proposed to ISF as improvement of SOGP, but this is not relevant to the research question of this MSc thesis.

The second row demonstrates a reasonable coverage between the BSR 6.3.1.1.1 requirement and the corresponding CB 2.2.6 in SOGP

The third row represents a BSR requirement that is not covered in SOGP but is considered as not relevant to a general standard.

The fourth row represents a requirement from SOGP of BSR that is relevant to the Bank and the research question and therefore should be included as a candidate for a topic in the metric. The term CB and a different numbering schema from BSR (CB6.1.1) can recognize such rows.

6.6 BSR and SOGP CB cross referenced to the Security analysis

In the content analysis of the Security analysis, we had already verified that the Security analysis was reasonably rooted on requirements in BSR.

The content analysis of BSR and the cross reference to SOGP gave a resulting table of requirements relevant to system development in the bank.

The next step was to cross reference the content of the Security analysis to the requirements and security topics in the table in order to verify that all requirements were properly addressed in the Security analysis.

The resulting cross-reference table would then be the basis for selecting the topics in the metric for “security status” as this has been defined earlier:

- The degree of compliance to the advice of solutions and requirements included in the Security analysis of the system
- The degree of compliance to (a subset of) the Bank’s BSR

Examples from the Cross-reference table:

Requirements in BSR cross ref to SA, SOGP AND METRIC IDEAS	**ISF SO GP Xref**	**COVER AND COMM.**	**SA Ref # TO INFO OR QUESTION**	**IDEAS FOR METRIC TOPICS IN SA-TOPICS (4.TH COLUMN)**
4.3.1.1.1 Suspicious incidents, threats and observed security violations in the data area must be reported, through the manager, to the IT-Security Department.	CB 2.4.1	3	57 IDS 58 IRT	Reporting of errors, security incidents, IRT
5.1.1.1.1 ✓ Each user must have a unique and personal UserID, which follows the standard of the Bank. The user must use the same UserID in all systems in the Bank.	CB 3.1.1 CB 3.1.3	4	5221 UserID std 19 Users IT platform (W2K or ACF2),	
5.1.1.1.2 Each user must have only one UserID to which all authorisation and privileges are related. Extra UserID or test-IDs must be approved for need by Central authorisation administrator (SA), and can only be used for the documented purpose.		3 “Only **one** UID” is not explicit	5221 UserID std	

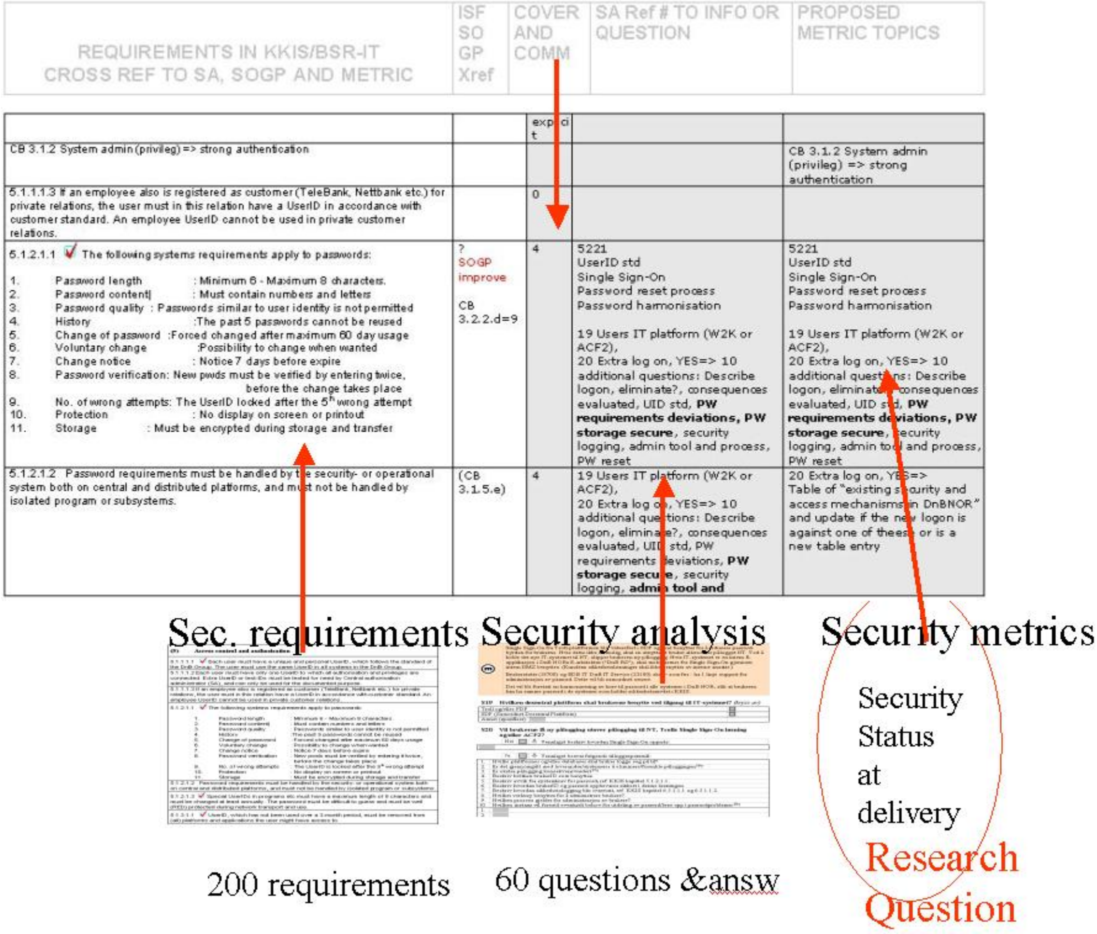
The 1. and the 2. column were explained in the section 6.5 *External validity: ISF's Standard of good practice* - *SOGP.*

The 3. column is an evaluation to verify that all requirements in the left column are properly addressed in the Security analysis (column four). The score is between 0 for no addressing to 4, which indicates a full coverage. The scores below 4 may be accompanied by comments to explain the reason as example in the 3. row shows: The requirement: “Each user must have only one UserID” is not explicitly covered but as this is implicit in the “5221 UserID standard” as this requirement will normally be ruled by the human control in the process for provisioning and administrating of UserIDs.

The 4. column is the content of the Security analysis: information given and questions asked (in keywords).

The 5. column was used to note ideas and inspiration from the conducted analyses. As the topics from the Security analysis in the fourth column would be obvious candidates, mainly ideas in excess of the fourth column were noted. Generally these ideas can be linked to the topics analysed or expressed in the other columns.

The resulting cross-reference table was then ready to be used as the basis for selecting the topics and defining the questions in the metric. The main source for the metric was the fourth and the fifth column with the other columns as reference of the intention and context of the security requirements that development projects must comply to.



REQUIREMENTS IN KKIS/BSR-IT CROSS REF TO SA, SOGP AND METRIC	ISF SO GP Xref	COVER AND COMM	SA Ref # TO INFO OR QUESTION	PROPOSED METRIC TOPICS
		explicit		
CB 3.1.2 System admin (privileg) => strong authentication				CB 3.1.2 System admin (privileg) => strong authentication
5.1.1.1.3 If an employee also is registered as customer (TeleBank, Nettbank etc.) for private relations, the user must in this relation have a UserID in accordance with customer standard. An employee UserID cannot be used in private customer relations.		0		
5.1.2.1.1 ✓ The following systems requirements apply to passwords: 1. Password length : Minimum 6 - Maximum 8 characters. 2. Password content| : Must contain numbers and letters 3. Password quality : Passwords similar to user identity is not permitted 4. History :The past 5 passwords cannot be reused 5. Change of password :Forced changed after maximum 60 day usage 6. Voluntary change :Possibility to change when wanted 7. Change notice : Notice 7 days before expire 8. Password verification: New pwds must be verified by entering twice, before the change takes place 9. No. of wrong attempts: The UserID locked after the 5^{h} wrong attempt 10. Protection : No display on screen or printout 11. Storage : Must be encrypted during storage and transfer	? SOGP improve CB 3.2.2.d=9	4	5221 UserID std Single Sign-On Password reset process Password harmonisation 19 Users IT platform (W2K or ACF2), 20 Extra log on, YES=> 10 additional questions: Describe logon, eliminate?, consequences evaluated, UID std, **PW requirements deviations, PW storage secure**, security logging, admin tool and process, PW reset	5221 UserID std Single Sign-On Password reset process Password harmonisation 19 Users IT platform (W2K or ACF2), 20 Extra log on, YES=> 10 additional questions: Describe logon, eliminate?, consequences evaluated, UID std, **PW requirements deviations, PW storage secure**, security logging, admin tool and process, PW reset
5.1.2.1.2 Password requirements must be handled by the security- or operational system both on central and distributed platforms, and must not be handled by isolated program or subsystems.	(CB 3.1.5.e)	4	19 Users IT platform (W2K or ACF2), 20 Extra log on, YES=> 10 additional questions: Describe logon, eliminate?, consequences evaluated, UID std, PW requirements deviations, **PW storage secure**, security logging, **admin tool and**	20 Extra log on, YES=> Table of "existing security and access mechanisms in DnBNOR" and update if the new logon is against one of theese or is a new table entry

Figure 23 BSR Cross reference

6.7 Work sheet for designing the security metric

As described, the Bank has a defined security process for system development and a security analysis to support this process. The Bank believes that this Security analysis will set a development project in a right direction, and clarify the main security considerations early in the project.

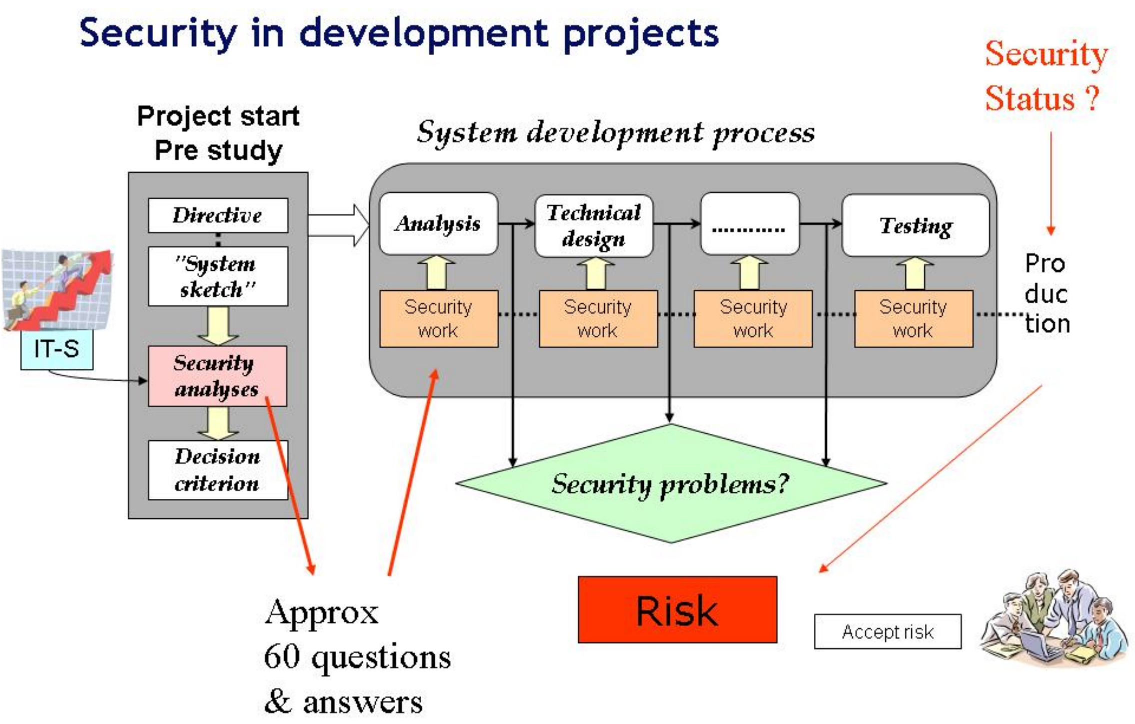


Figure 24 Security in system development

The problem is that we do not *know* what security related results this process and analysis tool is contributing with. We have no proof or measurement that a "good" Security analysis will result in a system that is secure by delivery.

The cross-reference table from the previous section gives a reasonable basis of candidates and topics for selecting the metric, but the table is in a BSR content structure.

The metric shall give a security status:

- The degree of compliance to the advice of solutions and requirements included in the Security analysis for the system
- The degree of compliance to (a subset of) the Bank's security requirements

The metric therefore has to follow the content structure of the Security analysis to ensure a clear link (line of sight) from the analysis to the metric and to reuse the work, answers and common grounds that the analysis has established between the project and the security department.

To assure a good linkage to the previous analysis steps, the content analysis of the Security analysis was combined with the right column of the cross-reference in a ”Security metric table”.

The presentation here is adjusted to the styles and page format of this report.

Security metric work table

#, SECTION & PURPOSE INFO GIVEN TO PROJECT	QUESTIONS IN SA	NEW METRIC	ANSW FROM SA	ANSW TO METR	TOPICS COPIED FROM CR REF IN EXCESS OF OR SUPPORT OF SA
5.3 Authentication, Authorisation and Access control for programs					
Recommended solution: - run as privileged service - access via program UID Must be registered in SLA for “Non personal UID”	34 Privileged service approved by responsible	34 privileged programs and TCB modifications: - registered - risk evaluation - approved by responsible		Yes=4	(9.2.2.4.1) privileged programs and TCB-modifications: - registered - risk evaluation
	35 Program UID via request process and SLA	35 Program UID via request process and SLA		Yes=4	
	38 New crypto keys or systems register in SLA	38 Are new crypto keys registered in SLA? 38.1 Is a new crypto system introduced? YES Is the new crypto system approved by ITS?		Y=4 Y+ Approved=4	7.2.5.1.1 ✓ Encryption solutions must be approved by the IT-Security Department prior to implementation

The table follows the structure and content of the Security analysis.

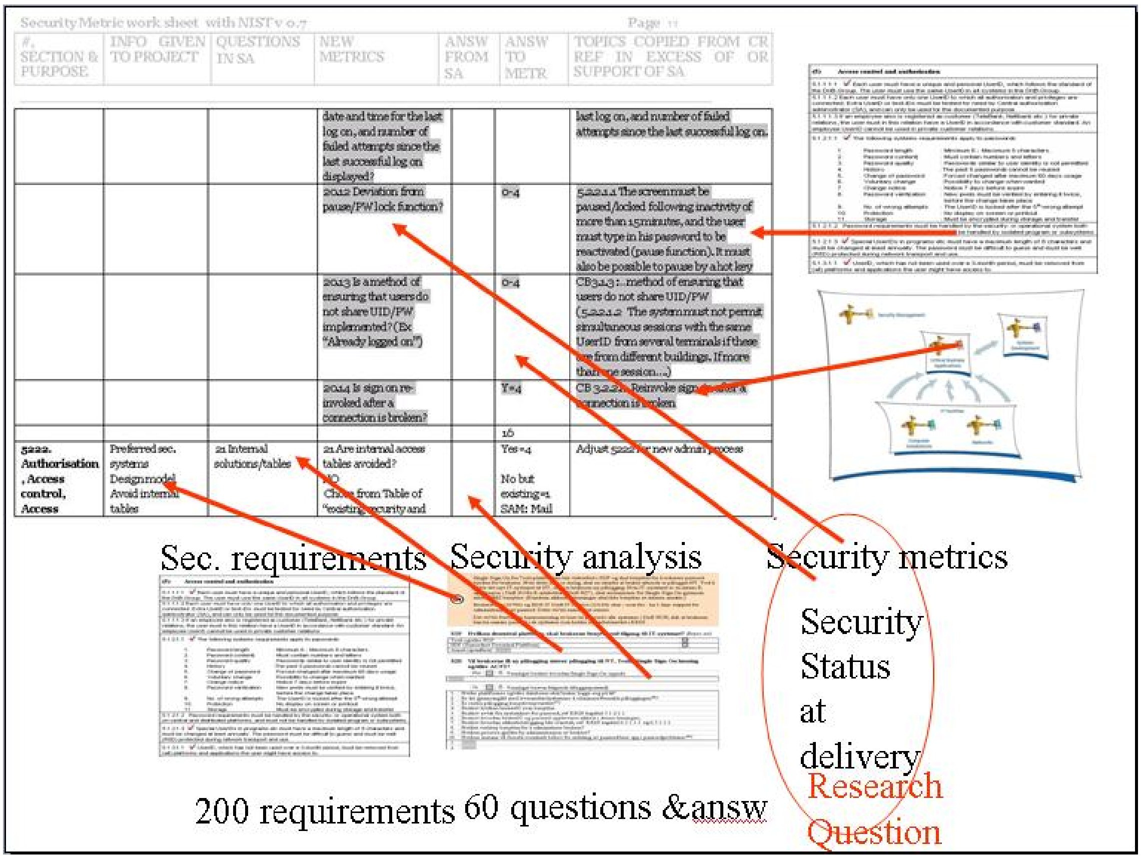
The 1. column is Section, purpose and information given and the 2. column are questions asked (in keywords) from the content analysis.

The 3. column is a proposal for the wording of the final metric. This may be a new wording or a new point of view for measuring the same topic as the example in the first row or a direct copy of the question asked in the Security analysis as the example in the second row. In many instances new questions were also added in the metric to clarify the security status, and the third row is an example of this.

The 4. column is reserved space for the answer given in the Security analysis.

The 5. column is a first try of setting a range for the metric: between 0-4 where 4 is full score. This will be described more closely in the next chapter.

The 6. column is the last column of the Cross reference described in the previous section: used to note ideas and inspiration from the previous analysis. As the topics from the Security analysis in the fourth column would be obvious candidates, only ideas in excess of the Security analysis were noted. As demonstrated in previous sections, these ideas can be linked to the topics analysed or worded in the analysed documents.



Security Metric work sheet with NIST v 0.7 Page 11

#, SECTION & PURPOSE	INFO GIVEN TO PROJECT	QUESTIONS IN SA	NEW METRICS	ANSW FROM SA	ANSW TO METR	TOPICS COPIED FROM CR REF IN EXCESS OF OR SUPPORT OF SA
			date and time for the last log on, and number of failed attempts since the last successful log on displayed?			last log on, and number of failed attempts since the last successful log on.
			2012 Deviation from pause/PW lock function?		0-4	5.2.2.1.1 The screen must be paused/locked following inactivity of more than 15 minutes, and the user must type in his password to be reactivated (pause function). It must also be possible to pause by a hot key
			2013 Is a method of ensuring that users do not share UID/PW implemented? (Ex "Already logged on!")		0-4	CB3.1.3 : ..method of ensuring that users do not share UID/PW (5.2.2.1.2 The system must not permit simultaneous sessions with the same UserID from several terminals if these are from different buildings. If more than one session...)
			2014 Is sign on re-invoked after a connection is broken?		Y=4	CB 3.2.2.1 Reinvoke sign on after a connection is broken
					16	
5222. Authorisation , Access control, Access	Preferred sec. systems Design model Avoid internal tables	21 Internal solutions/tables	21 Are internal access tables avoided? NO Chose from Table of "existing security and		Yes =4 No but existing=1 SAM: Mail	Adjust 5222 for new admin process

Figure 25 Security Metric work sheet

6.8 Considerations for the MSc thesis

At this stage we had a framework for the metric and we had a worksheet with candidates and inspiration for the content. We were ready to prototype the security metric and prepare for the first experimental use of it.

In this assignment we have prioritized to acquire and describe knowledge about security metrics by prototyping in a simple Microsoft Word table instead of time consuming programming in Microsoft Excel.

The complete metric prototype is given in Appendix B and has 116 topics to measure, but a typical system will not answer more then approx. 70 questions. This is due to the concept described in the section 2.2 *The control selection by application type*.

In the next section, we shall describe the testing and improvement of the metric.

For the sake of the reader of this report we have chosen a few metric topics and discuss them more thoroughly by means of 800-55 forms for each, describe in more detail the problems with logistics, source of answer, independent verification etc. instead of scratching the surface of the complete prototype with 116 topics.

7 Testing and improving the metric

7.1 Testing and developing the metric on the first system

7.1.1 Choosing a candidate

The following criteria for choosing a test candidate were defined:

- A system that has been exposed to a reasonable good Security analysis to give comparison between the measured values and the answers given in the corresponding Security analysis
- A system that is business critical or important enough to be worth the attention
- A system that has a scope broad enough to give measurement on all topics in the metric
- The participants should preferably have a need for the result of the metric

Ideally this should be a system that is "at delivery", but it may be difficult to find a suitable candidate when we need it. Instead we can choose a candidate that is in production, but then we have to eliminate possible errors stemming from the fact that the security status is not measured at delivery and may have been corrected.

7.1.2 The first test candidate

The system chosen is a human resource and salary system used in a specific part of the group.

Due to security reasons for the Bank, the system chosen cannot be described in detail, but will be described in general terms in order to demonstrate issues relevant to the metric.

The system is a standard system from the Service Provider and has not been designed to be compliant with the Bank’s standards and products or security requirements from the beginning of development.

The implementation project delivered the integration to the Bank’s environment last autumn and the system is in stable production.

We knew from a thorough Security analysis that the system had security deviations, but we did not know which problems the project actually had solved.

Logistics

The following logistics were found necessary to test and use the metric:

- To gather facts and documents on the system: responsible roles, Security analysis etc
- To arrange a meeting with the responsible roles to determine if they were interested in the results of such a metric and if it was possible to participate in this work now
- To perform the conversion of data from security analysis and other sources into the metric as a first draft
- To arrange a meeting in order to walk through the data and to confirm them as facts, define which topics need further investigation, and to define a process for the completion of the metric facts
- To arrange a meeting to analyse the non compliance areas, to evaluate risk and to formulate action plan for new controls or risk acceptance

This logistics is parallel to how the Security analysis or a standard Risk analysis is conducted.

In the case of this candidate, new persons had just been appointed to the responsible roles: System owner and Business owner and they were both interested in the result of the metric: the security status, so they would know which security problems and risks they had inherited from the project. The verification of certain technical facts still goes on. The samples given here is not necessary facts from the actual test, but may be constructed to illustrate.

The Risk Profile for the system

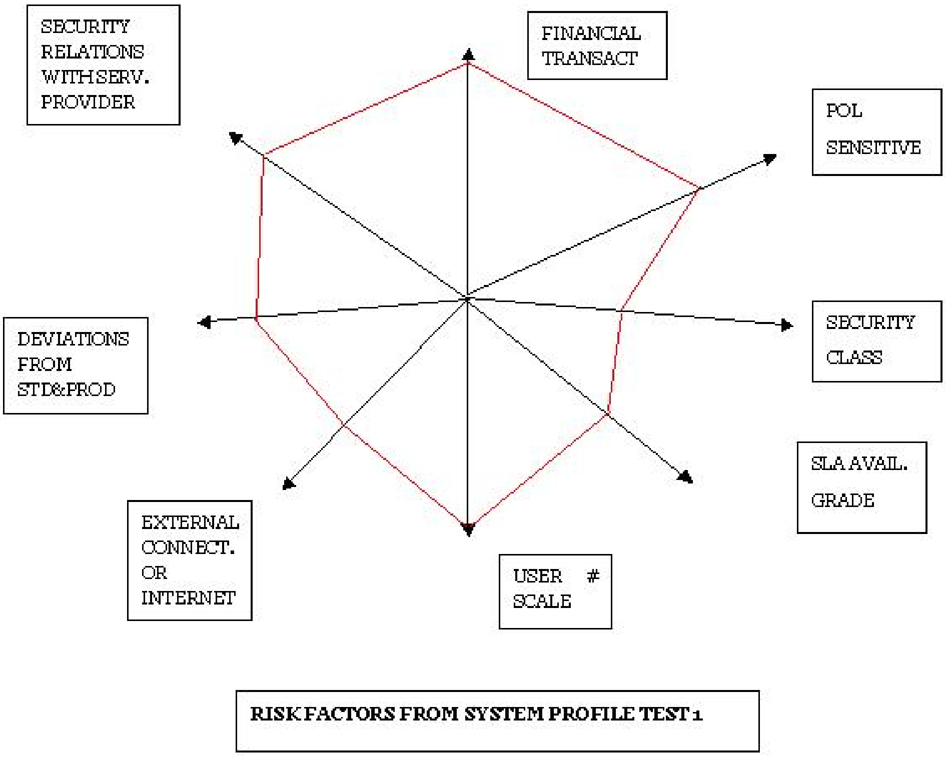

SECURITY RELATIONS WITH SERV. PROVIDER
FINANCIAL TRANSACT
POL SENSITIVE
SECURITY CLASS
SLA AVAIL. GRADE
USER # SCALE
EXTERNAL CONNECT. OR INTERNET
DEVIATIONS FROM STD&PROD
RISK FACTORS FROM SYSTEM PROFILE TEST 1

Figure 26 Risk factors from test 1

The Right side of the Spider diagram presents important risk factors from a business point of view. By presenting them together, they may show inconsistence. The more spread they are, the greater the business need for compliance to security relevant for the factors.

RISK ASPECT	EXPLANATION	RELEVANCE / COMMENTS HERE
Financial Transaction	If a system in a bank can participate in Financial transactions, it has a risk of fraud.	The salary system pays out large batch files of salary and there is a risk of fraud through false employees, salaries or fraudulent batch files.
POL[36] sensitive	The Norwegian Privacy act – POL [36] – defines certain info as Sensitive which requires stronger security measures regarding confidentiality	The human resource system has diverse info on each employee that is considered private. It also contains fields like "Union member" that is labelled Sensitive by POL [36]. It is unclear and debated in the HR section[7] if the full requirements of POL Sensitive come into place.
Security class	The Security analysis requires the system to be risk analysed and classified with respect to CIA.	The class given is Blue=Medium Security in regards to CIA.
SLA availability grade	The SLA Availability grade for the system indicates the business importance of availability and increase in risk of disruptions.	The SLA Availability grade is B, which indicates medium requirements for availability in terms of opening hours.
User # scale	User # scale indicates if the system is used by a small or large number of users.	The number of users includes all employees (12000) as they are required to update certain information on education, absence (holidays, illness etc) and can look at all info the system has stored on the employee

The Left side of the Spider diagram presents important risk factors from a technical point of view. By presenting them together with the business point of view, they may indicate a threat level that needs special attention and stronger security controls.

[7] Human Resource division

RISK ASPECT	EXPLANATION	RELEVANCE / COMMENTS HERE
External connections or Internet	The potential risk increases if the system has external connections, has external users and even more if the system is to be used over the Internet	The Service provider is external (to the main Service provider). The users will use Web over extranet.
Deviations from Standards and products	The potential risk increases if a system is built on “new” technology that has never been analysed before. This also often excludes the recommended security solutions as they may not be supported in this environment	The system is a standard system from the SP and has never been designed to be compliant with the Bank’s standards and products or security requirements.
Security Relations with the Service Provider	The potential risk increases if the SP is “New”, is unfamiliar with the Bank’s Security Requirements and the contractual security obligations are weak.	There are only a few words in the existing contract regarding security. A security appendix is now required for contracts with external SP and lays the ground for a structured and measured relation with the SP.

Selected samples from use of the metric

To illustrate how the Metric prototype is designed, we use selected examples from this system candidate.

Security Relations with the Service Provider

As explained in “The Bank’s approach to security”, compliance to standardized security solutions is an essential strategy.

The Bank’s IT Operations are outsourced to one major vendor and there are established clear agreements regarding delivered services. A “Vendor management” section in the Bank is responsible to follow up, measure and sanction that the Service Provider (SP) is performing according to the contract.

The Bank has decided that this SP will be the first choice for all new systems to achieve advantage of scale.

Security is integrated in this model and the IT Security department is participating in defining, measuring and sanctioning the SP’s security performance. This is described in [3]. There is a dedicated person in the IT security section that is responsible for Vendor Security management.

In the Security analysis it is assumed that this main SP is used and Question 65 test if the relevant security roles at the SP have participated in evaluating operational and system technical security issues in the project. The role “Service planner” is the SP's representative in the project and is required to orchestrate these evaluations bringing in the necessary roles and expertise with knowledge of the Bank's BSR and recommended solutions.

The problem is that when an SP different from the main one is used – as in this case – we cannot assume that this model is working. There may not be an agreement in place that defines this security model. To test how much of this model that is in place, we have proposed a new series of questions along the lines in NIST 800-55 called "Implementation evidence".

The first question – 65.1 - is a "routing question" to test if another than the main SP is used. If NO then we can skip the rest of the questions because the model is in place. If the answer is Yes then each question tests closer and closer to the model and "Security relations" that we have with the main SP.

In this case the answer to 65.1 is Yes which means "other SP then the main one". Question 65.2 tests if there is an agreement with a standard security appendix and the answer is NO. The information: "The Security department has a standard security appendix that should be used" is a remark to suggest a solution to the non compliance.

As demonstrated there is no sense in continuing with the other questions in this series because the SP is not required to comply with the security model.

SECTION, PURPOSE & INFO NEW METRIC	ANSW ALT. TO METR	TEST OF METRIC I.e.: TEST 1 INFO FROM SA + METRIC ANSWERS
65 Security remarks from external Service provider (via Service planner)	Y=4	
65.1 Is the system operation outsourced to other Provider then the main Service Provider? IF YES:	Y=0	Y=0
65.2 Is there an agreement with a standard IT security appendix?	Y=4	NO=0 The Security department has a standard security appendix that should be used to amend this.
65.3 Is the agreed security performance reported and controlled 2 times a year?	Y=4	
65.4 Are the Providers people appointed to the relevant roles in writing?	Y=4	
65.5 Are these roles quality assuring the measurements in this metric?	Y=4	
65.6 Is the Service planner contributing to security on behalf of Provider?	Y=4	

For illustration we describe this security topic in NIST800-55 form.

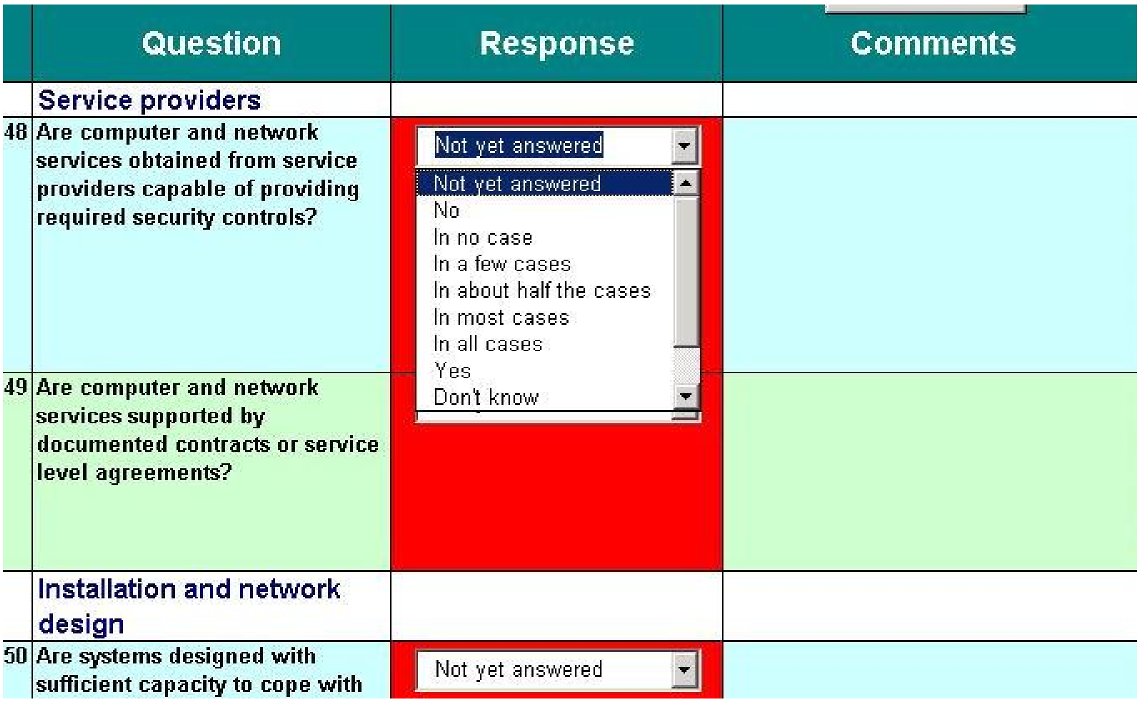
The Metrics detail Form from 800-55		**Description for Q 65.- Security Relations with SP**
Performance Goal	State the desired results of implementing one or several system security control objectives/techniques that are measured by	The desired result is to assure that the SP is legally bound to deliver a secure service as

The Metrics detail Form from 800-55		**Description for Q 65.- Security Relations with SP**
	the metric. When using NIST SP 800-26, this item will list a critical element, as stated in 800-26.	specified and that the SP's security performance is measured and sanctioned.
Performance Objective	State the actions that are required to accomplish the performance goal. When using NIST SP 800-26, this item will list one or more subordinate questions, as stated in 800-26. Multiple performance objectives can correspond to a single performance goal.	The actions required are to include the Security appendix to the agreement with the SP and arrange for measurement and sanctioning.
Metric	Define the metric by describing the quantitative measurement(s) provided by the metric. Use a numeric statement that begins with the words "percentage," "number," "frequency," "average," or other similar terms.	The metric will uses a number in a range from 0 – 4. Here it is expected to be either 0 for non-compliance or 4 for full compliance but the range is to indicate partial compliance. The special case of 65.1 where Yes gives the score = 0 is explained after the table
Purpose	Describe the overall functionality obtained by collecting the metric. Include whether a metric will be used for internal performance measurement or external reporting, what insights are hoped to be gained from the metric, regulatory or legal reasons for collecting a specific metric if such exist, or other similar items.	The purpose here is to be able to manage the security of outsourced contracts without getting into all technical details in the metric, which is the business and system owner's view.
Imple-mentation Evidence	List proof of the security controls' existence that validates implementation. Implementation evidence is used to calculate the metric, as indirect indicators that validate that the activity is performed, and as causation factors that may point to the causes of unsatisfactory results for a specific metric. (Original NIST parenthesis removed)	The evidence that the SP in "Security relations" is indicated by the series of questions in 65, each question tests closer and closer to the model and "Security relations" that we have with the main SP.
Frequency	Propose time periods for collection of data that is used for measuring changes over time. Suggest time periods based on likely updates occurring in the control implementation. (Section 4.3, Feedback Within Metrics Development Process, contains a discussion	The frequency – for all aspects in the metric - will be the same. The complete metric, or a subset, will be used at system delivery on demand

The Metrics detail Form from 800-55		**Description for Q 65.- Security Relations with SP**
	on the frequency of metric data collection.)	
Formula	Describe the calculation to be performed that results in a numeric expression of a metric. The information gathered through listing implementation evidence serves as an input into the formula for calculating the metric.	The questions are generally answered as described in the Metric row: as 4 or 0, but may be evaluated to a number in between to indicate partial compliance.
Data Source	List the location of the data to be used in calculating the metric. Include databases, tracking tools, organizations, or specific roles within organizations that can provide required information. (Section 3.4.3, Data Management Concerns, contains a discussion on metrics data sources.)	The main data source will be the Agreement with the SP, but the System owner must also confirm that arrangements for measurement and sanctioning are in place.
Indicators	Provide information about the meaning of the metric and its performance trend. Propose possible causes of trends identified through measurement and point at possible solutions to correct the observed shortcomings. State the performance target if it has been set for the metric and indicate what trends would be considered positive in relation to the performance target. (Section 4.2, Establishing Performance Targets, contains a discussion about the relationship of performance targets and the indicators.) Describe how the information gathered through listing implementation evidence is to be used as input into the analysis of indicators. The implementation evidence serves for validating performance of security activities and pinpointing causation factors	One should have special attention if the person in the IT security section that is dedicated to Vendor Security management is not informed or involved in the measurement process for a particular vendor or system. Extra implementation proof should be sought to verify that the Security appendix is really enforced or if the model is not functioning. The lack of skills in security and vendor management may pose a problem.

A comparison to ISF Security Health check

The Health check has a question in the same area, but it asks if the SP is *capable of providing the required Security controls.*



	Question	Response	Comments
	Service providers		
48	Are computer and network services obtained from service providers capable of providing required security controls?	Not yet answered	
49	Are computer and network services supported by documented contracts or service level agreements?		
	Installation and network design		
50	Are systems designed with sufficient capacity to cope with	Not yet answered	

Figure 27 ISF: Sample from Health Check

It is obvious – by looking at the question and the answer alternatives - that the reliability may be an issue, but we must remember that this is a metric checking at a high level and at a full range of security aspects and sections in SOGP. As our Security metric is measuring on a limited range we can go deeper on each subject. The ISF Survey goes into even more details on the same topic.

If the comments in the last column in the Health check explain the non-compliance, then it may be less important if the score is 2 or 3.

We think that the reliability of ISF metrics can be improved by adding information like Proof of implementation, but this again may increase the workload of the metric.

Should one formulate negative or positive questions regarding compliance?

The problem is illustrated in Q65.1 where one asks for *non*-compliance to the model: "outsourced to other Provider then the main SP".

65.1 Is the system operation outsourced to another Provider then main Service Provider? IF YES:	Y=0	Y=0
65.2 Is there an agreement with a standard IT security appendix	Y=4	

The question could have been turned to "compliance" by asking if the main SP is used. This may look more logical in the metric by giving Y=4 instead of Y=0.

The Security analysis uses a combination of positive and negative questions regarding compliance, and the main reason has been to formulate the question in the way that best explains or focuses on the problem, and make the user understand the consequences of non-compliance.

Because this is already an issue in the Security analysis, we have not made a strong case for which is the best, but it leads to some logic problems in using the metric. This should be decided by the Bank for both the Security analysis and the metric, and will be listed in further work.

7.2 Analysing the result and improving the metric

As shown in the previous section, some analysis of the facts has been concluded and some are still ongoing regarding the system Candidate 1.

The special challenge regarding the metric was that the prototype metric was actually developed during this first measurement.

As a starting point we had the resulting Security Metric work sheet from the previous chapters.

We started by copying the information from the Security analysis. The direct number relation between the Security analysis and the metric was very important in doing this, but there were several obstacles:

- Inaccurate translation from Norwegian had to be corrected
- Converting security keywords from previous analyses into reasonable and logical questions
- Change of structure or content from Security analysis had to be justified
- The new questions in the metric had to be positioned logically in the Security analysis structure

The metric should- as a total - make sense from the point of view of a system owner that had never seen the metric before, but was well acquainted with the Security analysis.

The feedback from the first system owner was invaluable as we went through the content of the metric. By luck she had an English heritage and could easily work back and forth between Norwegian documents and an English Metric (provided the necessary assistance).

7.3 To measure and analyse the next candidate

7.3.1 The second test candidate

The system chosen is an international payment system, which is core business to the Bank.

Due to security reasons for the Bank the system chosen cannot be described in detail but will be described generically here to demonstrate issues relevant to the metric.

The system is a partly a standard system from an external development vendor but the project delivers a totally integrated and customized system that will be operated by the standard SP. The development vendor knows the Bank’s security model and the system have been designed to be compliant with the Bank’s standards & products and security requirements from the beginning.

We knew from a thorough Security analysis that the system should have few non-compliance areas, but we wanted to use the metric to assure that all problems addressed had actually been solved by the project.

The project state was ideal as the system was put in production, security facts was available, but the project had a few months more to deliver all agreed details.

Logistics

We followed the logistics established with the first candidate:

- To gather facts and documents on the system: responsible roles, Security analysis etc
- To arrange a meeting with the responsible roles to check if they were interested in the results of such a metric and if it was possible to participate in this work now
- To do the first conversion of data from security analysis and other into the metric as a first cut
- To arrange a meeting to walk through the data and to confirm this as facts, define which topic that need further investigation, and to define a process for the completion of the metric facts
- To arrange a meeting to analyse the non-compliance areas, to evaluate risk and to formulate action plan for new controls or risk acceptance.

In this case the responsible roles: Project manager and the future System owner were both interested in the result of the metric: a security status so they would know which eventual security problems and risks that existed at delivery from the project. The verification of facts still goes on, but some facts are concluded and can be presented here.

The Risk Profile for the system

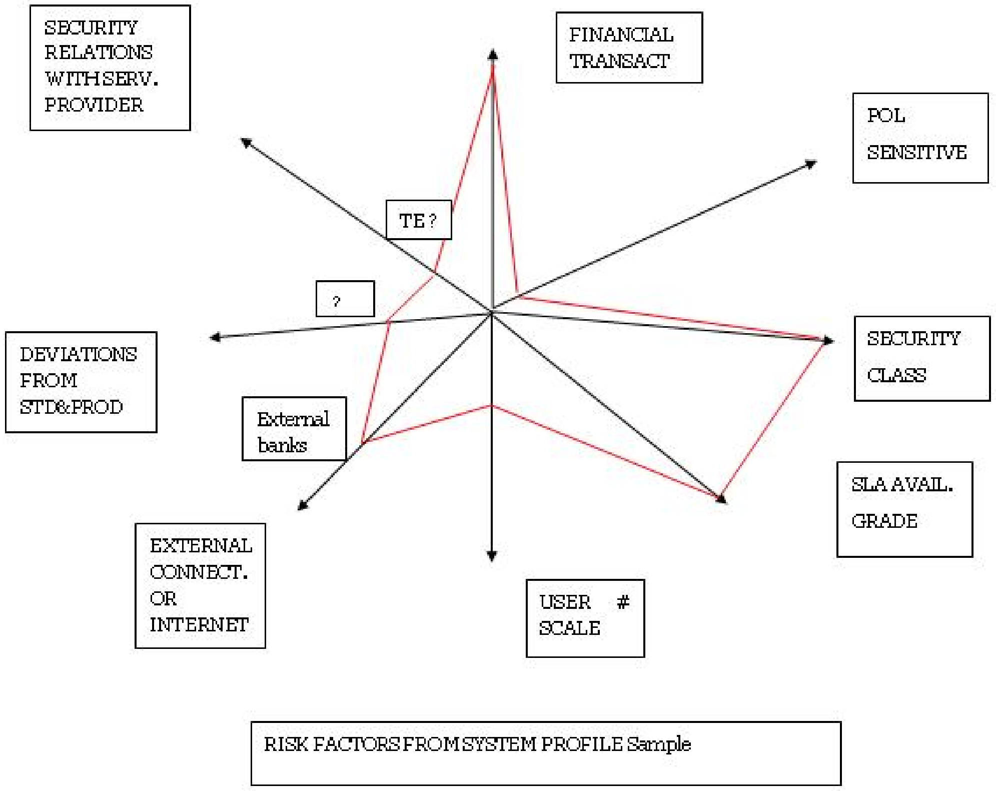


Figure 28 Risk profile second candidate

The Right side of the Spider diagram presents important risk factors from a business view. By presenting them together, they may show inconsistence. The more spread they are, the greater the business need for compliance to security relevant for the factors.

RISK ASPECT	EXPLANATION	RELEVANCE / COMMENTS HERE
Financial Transaction	If a system in a bank can participate in Financial transactions, it has a risk of fraud.	The international payment system handles large sums and there is a risk of fraud through false or fraudulent international payments.
POL[36] sensitive	The Norwegian Privacy act – POL – defines certain info as Sensitive which requires stronger security measures regarding confidentiality	The payment system has a normal customer database and has no data classified as Sensitive in POL [36].
Security class	The Security analysis requires the system to be risk analysed and classified with respect to CIA	The class given is Red= High Security in regards to CIA where the highest scores came from Availability followed by Integrity.
SLA availability grade	The SLA Availability grade for the system indicates the business importance of availability and increase in risk	The SLA Availability grade is A which indicates that it has the highest requirements for availability regarding 8700 opening hours pr year.
User # scale	User # scale indicates if the system is used by a small or large number of users and therefore if logon and access admin are critical issues	The number of users are medium (a few thousand) but also includes employees in > 100 external banks where the Bank act as service provider.

The Left side of the Spider diagram presents important risk factors from a technical point of view. By presenting them together with the business point of view, they may indicate a threat level that needs special attention and stronger security controls.

RISK ASPECT	EXPLANATION	RELEVANCE / COMMENTS HERE
External connections or Internet	The potential risk increases if the system has external connections, has external users and even more if the system is to be used over the Internet	The external banks are connected through extranets. The system is not exposed to Internet. The system has several external connections to high risk backend systems (i.e. BBS and Swift)
Deviations from Standards and products	The potential risk increases if a system is built on “new” technology that has never been analysed before. This also often excludes the recommended security solutions as they may not be supported in this environment	The system is a standard system from the SP but has been designed to be compliant with the Bank’s standards and products, security requirements and recommended solutions to a reasonable degree, due to long term relations with banks.

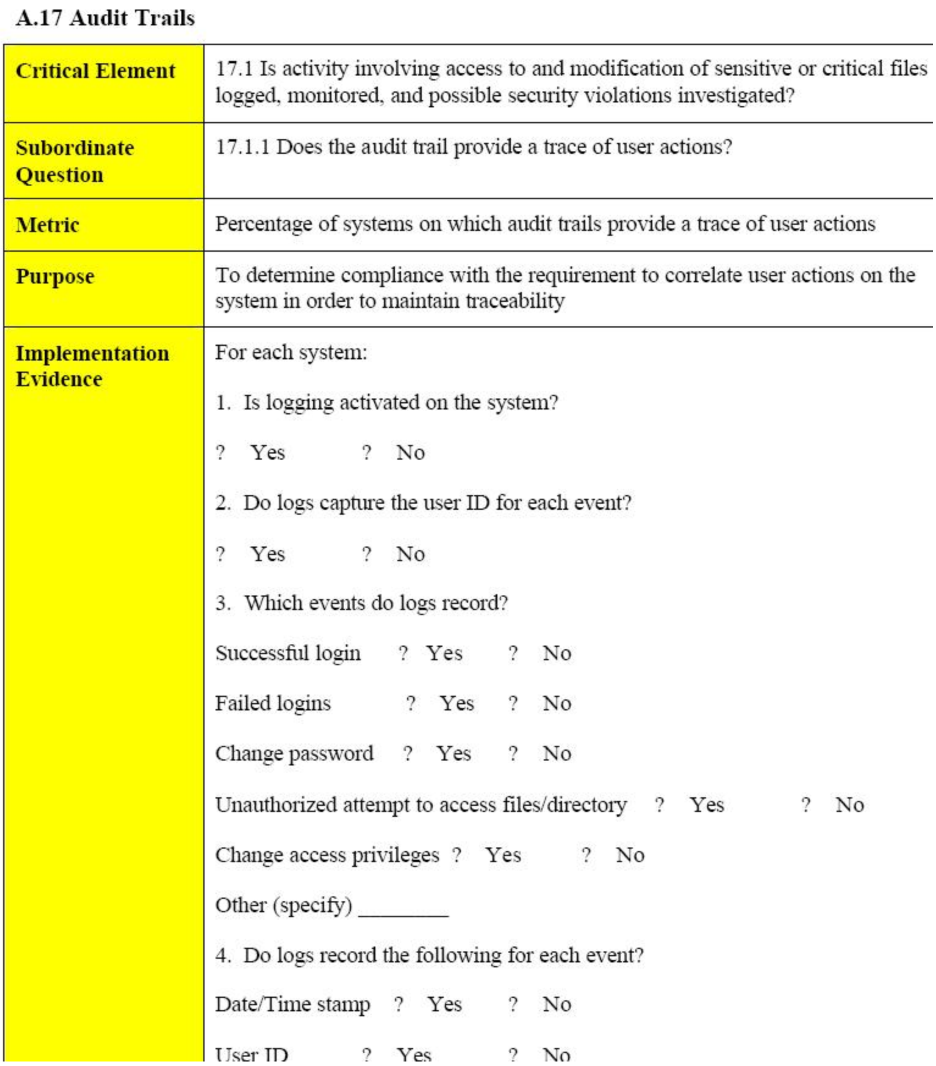
Security Relations with the Service Provider	The potential risk increases if the SP is "New", is unfamiliar with the Bank's Security Requirements and the contractual security obligations are weak.	There is a reasonable security section in the agreement with the development company. A security appendix should be added to the contract with external SP to lay the ground for a structured and measured relation with the SP regarding the future **development and maintenance** of the system. The **operation** of the system is outsourced to the standard SP and follows the security model.

Selected samples from use of the metric

To illustrate how the Metric prototype is designed, we use selected examples from this application as illustration.

Security audit trail

Here we compare a sample metric from NIST with the same topic in the metric.



A.17 Audit Trails

Critical Element	17.1 Is activity involving access to and modification of sensitive or critical files logged, monitored, and possible security violations investigated?
Subordinate Question	17.1.1 Does the audit trail provide a trace of user actions?
Metric	Percentage of systems on which audit trails provide a trace of user actions
Purpose	To determine compliance with the requirement to correlate user actions on the system in order to maintain traceability
Implementation Evidence	For each system: 1. Is logging activated on the system? ? Yes ? No 2. Do logs capture the user ID for each event? ? Yes ? No 3. Which events do logs record? Successful login ? Yes ? No Failed logins ? Yes ? No Change password ? Yes ? No Unauthorized attempt to access files/directory ? Yes ? No Change access privileges ? Yes ? No Other (specify) ________ 4. Do logs record the following for each event? Date/Time stamp ? Yes ? No User ID ? Yes ? No

Figure 29 NIST 800-55 sample Audit trail

SECTION, PURPOSE & INFO **NEW METRIC**	**ANSW** **ALT. TO** **METR**
5.7 Audit, logs and Incident handling Relates to 5.2.2 United Time Code UTC for synchronised clocks 2 independent logs A coherent log chain as evidence	
70 Are clocks for logging synchronised with deviations > 2 seconds from time Norwegian std time with NTP/UTC or similar?	NTP/UTC=4
71 Is a consistent log chain between Bus.log <> sec.log tested? Is a desk-test of “false transaction complaint” with use of logs performed?	Desk test performed =4
71.1 Are there two independent logs in the chain?	Y=4

SECTION, PURPOSE & INFO **NEW METRIC**	**ANSW ALT. TO METR**
(Independent means that collusion is necessary to forge both logs identical)	
71.2 Deviations from bus and sec log record std content #62112, successes #65111 or violations #65112?	No=4
71.3 Is log data on line > month, easily available, and kept for min 13 months	Y=4
71.4 Are controls of logs conducted to prevent and discover unauthorised access?	Y=4
57 IDS sensors Are HIDS / NIDS sensors giving the application adequate protection?	Y=4
58 IRT Info Is Info and Reporting of errors and security incidents described and agreed with IRT in the Bank? Is the vendor's IRT operational regarding this system?	Y=4
58.1 Agreed with IRT how logs can be consolidated?	Y=4

A comparison:

In the NIST sample the detailed log content requirements are listed as checkpoints in Implementation evidence.
We have chosen to refer to the Bank’s security requirement in 71.2 "... log record std content #62112, successes #65111 or violations #65112", which defines similar requirements of which incidents, and actions should be logged.

We want to keep the metric at a level higher on this topic:

- To avoid repeating details given in the requirements to assure that the user of the metric also has to know the content of BSR – not only the metric or the Security analysis
- To allow for adjustment of the detailed requirements without having to rewrite the metric
- To use the same number of questions to test a broader range of "Audit trail" related topics:
    - To see several log types from more than one platform in a coherent view by consolidating and synchronising them to a "log chain" – also synchronized in exact time
      This log chain should be admissible as evidence in court
    - To use this in context with IDS where host IDS often is working on the same log files
    - To see this in conjunction with local and central Incident Response Teams to react on incidents in the logs

For illustration we describe this security aspect in NIST800-55

The Metrics detail Form from 800-55		**Description for the Q – series of 5.7 Audit, logs and incident handling**
Performance Goal	State the desired results of implementing one or several system security control objectives/techniques that are measured by	The desired result is to assure that logs, audit and incident handling is covering

The Metrics detail Form from 800-55		**Description for the Q – series of 5.7 Audit, logs and incident handling**
	the metric. When using NIST SP 800-26, this item will list a critical element, as stated in 800-26.	the Bank's need to document how the customers financial assets were handled
Performance Objective	State the actions that are required to accomplish the performance goal. When using NIST SP 800-26, this item will list one or more subordinate questions, as stated in 800-26. Multiple performance objectives can correspond to a single performance goal.	The actions required is to verify that the transaction path is recorded and that the supporting systems and organisation will react on security events to produce a log chain admissible as evidence of incidents
Metric	Define the metric by describing the quantitative measurement(s) provided by the metric. Use a numeric statement that begins with the words "percentage," "number," "frequency," "average," or other similar terms.	The metric will use a number in a range from 0 – 4. Here it is expected to be either 0 for non-compliance or 4 for full compliance but the range is to indicate partly compliance.
Purpose	Describe the overall functionality obtained by collecting the metric. Include whether a metric will be used for internal performance measurement or external reporting, what insights are hoped to be gained from the metric, regulatory or legal reasons for collecting a specific metric if such exist, or other similar items.	The purpose is to enforce accountability for the users and customers own actions and comply to legal requirements of audit trail in accounting
Imple-mentation Evidence	List proof of the security controls' existence that validates implementation. Implementation evidence is used to calculate the metric, as indirect indicators that validate that the activity is performed, and as causation factors that may point to the causes of unsatisfactory results for a specific metric. (Parenthesis in original text is removed)	The evidence is built on testing a broad range of questions in the section. The answer alternative to Q70 and indicate the preferred answer/evidence for a full score. If this is not the case then the assessment of implementation is more open
Frequency	Propose time periods for collection of data that is used for measuring changes over time. Suggest time periods based on likely updates occurring in the control implementation. (Section 4.3, Feedback Within Metrics Development Process, contains a discussion on the frequency of metric data collection.)	The frequency – for all aspects in the metric - will be the same. The complete metric, or a subset, will be used at system delivery on demand

The Metrics detail Form from 800-55		**Description for the Q – series of 5.7 Audit, logs and incident handling**
Formula	Describe the calculation to be performed that results in a numeric expression of a metric. The information gathered through listing implementation evidence serves as an input into the formula for calculating the metric.	Each question will have its own evidence and will indicate the area of non-compliance by a lower score then 4.
Data Source	List the location of the data to be used in calculating the metric. Include databases, tracking tools, organizations, or specific roles within organizations that can provide required information. (Section 3.4.3, Data Management Concerns, contains a discussion on metrics data sources.)	The main data source can be the section of the test report testing logs and IDS and confirmation from IRT responsible that necessary information has been given
Indicators	Provide information about the meaning of the metric and its performance trend. Propose possible causes of trends identified through measurement and point at possible solutions to correct the observed shortcomings. State the performance target if it has been set for the metric and indicate what trends would be considered positive in relation to the performance target. (Section 4.2, Establishing Performance Targets, contains a discussion about the relationship of performance targets and the indicators.) Describe how the information gathered through listing implementation evidence is to be used as input into the analysis of indicators. The implementation evidence serves for validating performance of security activities and pinpointing causation factors	One should have special attention if the system has Yes in Question 65.1 "Is the system operation outsourced to another Provider then main (SP1)?" Extra implementation proof should be sought to verify that the topics in this section are functioning as a complete security chain (I.e. sync of clocks between SPs). The lack of skills in security and vendor Security management may pose a problem. The lack of coherent logs as admissible proof in court may not be discovered before the first serious incident.

8 Analysing the thesis's work and findings

The research question is how to define a security metric that measures the security status of a new system at delivery in an objective and concise manner.

The term *security status* can be defined from different points of view:

- The degree of compliance to the advice of solutions and requirements included in the Security analysis for the system
- The degree of compliance to (a subset of) the Bank's security requirements
- To explain the security status and area non compliance in terms of the business need for Confidentiality, Integrity and Availability

The scope of the *security status* must be decided in the thesis from a reasonable combination of these points of view.

8.1 Evaluating the metric

The following issues were analysed:

- Value of the measurement to the bank
- Validity
- Reliability
- Sound scientific foundation
- The workload of measuring

Value of the measurement to the Bank

As described earlier, the Bank's value from the metric is not an isolated score. The real value for the Bank lies in collecting security facts and evaluating risk associated with the low scores.

Even with a premature prototype in the first test, we had valuable discussions on non-compliance areas that were fresh to the newly appointed System owner. She welcomed the oversight it gave her and has set a meeting to discuss facts and potential improvements with the Service Provider. After all – Risk management and Security processes are only worthwhile if they lead to measurable improvement. When this metric leads to improvement, we can easily document which areas that has been improved.

The metric strengthens the existing process for the Security analysis by giving a tool to follow up the security decisions made earlier in the project and lead them through to results.

Validity

The internal validity of the metric is fair as it is measuring compliance as needed. The metric is built on the same structure and numbering schema as the Security analysis and the cross-references conducted leads to a reasonable and traceable coverage of the Bank's security requirements.

The external validity in terms of a metric that can be applied to other businesses and contexts is a debatable one. The security approach and documents are proprietary to the Bank, and the content has to be adjusted to other requirements to meet other business needs. Cross-referencing to SOGP CB as described in an earlier chapter indicates external validity.

The knowledge on designing metrics described in this report we believe has external validity and this is focused in the section *How to generalize the metric.*

Reliability

The reliability can be a major challenge in Security metrics because there often are elements of assessment and interpretation in deciding the measurement for a complex security issue. This is not unique to this prototype metric and is demonstrated in an example from ISF Security Health check. It is also well known to the Bank with the Security analysis and the ISF Survey.

On the other hand, if the metric cannot – on the average - establish facts about the security status and area of non-compliance of a system, then it has failed.

The final metric should state how the person using the metric could assure that each value in the metric is correctly assessed – ".. in an objective and concise manner". The ultimate "seeing is believing" will generate more work - and maybe an unrealistic effort of testing – to establish the proof we ask for.

In the prototype we have designed each question or series of questions with the intention to document "implementation evidence". We have also tried to give answer alternatives as "algorithm" to set the value of measurement based on implementation facts as described in NIST Sample metrics [4]. This work should be improved as the Bank finalizes a Norwegian metric.

We need to balance the scientific need for accuracy and the business need for a manageable workload of measuring. Testing the metric by using different persons measuring the same system can indicate the reliability. But we must keep in mind: the real value for the Bank lies in collecting security facts and do risk evaluation of the low scores, not the detailed accuracy of the score. The process of assessing security will have a value of its own.

A partial solution to the reliability problem with security metrics is to use the same person or a small group of trained people as consultants when the metric is used. This can ensure a consistent understanding and use of the metric, reduce the need for lengthy, precise instructions to the user and reduce the possibility of a bias.

For the Bank it may be natural to use dedicated security consultants to supervise the use of the metric and to quality assure the measurements. Tools like Security analysis, Risk analysis and others are already conducted with dedicated consultants.

If an IT-based tool can support the metric, the reliability can be increased by:

- Assisting the user in using the process and tool correctly
- Giving easy access to relevant explanations and requirements to understand the context of each question
- Calculating more complex scores based on the answers (proof of implementation) in a series of related questions
- Copying data automatically and correct from Security analysis to correct field in Security metric
- Collecting data from i.e. predefined test, macros or sources

This will certainly also reduce the workload of measuring, and move the focus from collecting to analysing and improving security.

Sound scientific foundation

The principles used for this metric are taken from literature and industry that represent best practice. If we take into account that the field of measuring Security is immature and that structured metrics are scarcely used, there is not much empiri to support the scientific principles [13]. The metrics in most extensive use in the industry is probably ISF metrics and we have built our metric on ISF principles.

The workload of measuring

If the Metric were a stand-alone tool, the workload of using it would have been substantial. As the metric is closely building on a workload already conducted – Security analysis, the extra workload should not be substantial.

The Project manager is responsible for making the system compliant with the Bank's security requirements by implementing and documenting security - not only analysing security.

The experiments we have done with the metric indicate some important points:

- If the metric is used by a project *in the delivery phase*, the knowledge of Security analysis, compromises made and areas of non-compliance is available in the project. One can move quicker from the fact gathering/data collection to analysing the measurement
  The second test candidate was an example of this setting
- If the Project manager knew from the start of the project that the metric should be used at delivery, it may reduce the workload substantially by collecting the specified "implementation evidence" as part of testing and documenting the system
- If the metric is used by the System owner / Business owner to document security facts of a system *long after the delivery project is closed* and project members have lost touch with the system, the fact gathering gives more workload.
  The first Candidate was an example of this setting.

The workload is also closely connected to the discussion of reliability above. We need to balance the scientific need for accuracy and the business need for a manageable workload of measuring.

We will also recommend an IT-support for the Security analysis and the related metric in the section: *Further work.*

8.2 The secondary purpose of the metric

The secondary purpose of the metric is to indicate the effect of the security process, indicate areas of improvement and to enlighten which area and topics in the process and analysis that needs improvement.

The main source for this will be the analysis of the root cause of the areas of non-compliance, but we also may need some information of the projects perception of the Security analysis and the associated process.

To assist this we have developed a prototype questionnaire to capture this perception. It has samples from one of the systems that were measured.

TOPIC	TRIGGER QUESTIONS	ANSWERS & COMMENTS
Quality of SA process and dialogue	- Dialogue with ITS from start of project? - SA formally evaluated by ITS before project 50% finished?	Yes, but contract was signed with external vendor before Security analysis No, 1. meeting 26/8 and production date only two months later - October (?)
Experience with SA Indicates how SA is contributing and how the process is perceived	Where do we need improvement of SA or the security process of system development What was the least valuable?	The Security Analysis does not give a clear support for this type of project: external system for Internal users, and should be improved.
Clarity	Describe SA questions or topics that needs further explanation or rephrasing	
Security architecture and solutions	Where do we need improvement of Security Vision, Architecture, solutions or Security processes presented in SA	Needed assistance from ITS defining a workable solution to SSO for external SP's
Root cause	Describe the root cause of the major non compliance areas	Contract was signed by director X with external vendor before Security analysis and minimal Security obligation in contract
Workload	Was the recourses spent on Security > 2% of the total budget?	
	How much time spent with Security analysis? What was most time-consuming?	
Other	Problems relating to other issues	

This questionnaire is just an untested prototype and must be finished by the Bank in Further work.

8.3 The Authors role

In the chapter 4 *Choice of methods* we described the possible bias of the Author on two areas:

- The risk of being too involved in the documents involved to be objective
- The risk that the proprietary setting – from a scientific point of view - may lead to a “home grown *suggestion* of a metric” instead of achieving new general knowledge on metrics

Objectivity – the risk of being to involved

The Author has been the main author of the Security Requirements document and a strong contributor to the Security analysis, which constitute the basis for the metric. There may be a risk that the Author may be biased and may try to design a metric that is self-evident, by giving unconscious credit to previous work or avoiding weak areas.

To compensate for this the Author has arranged for a Reference group of internal experts in the field of System developments and security to oversee and approve the selection of parameters and the development of the metric.

The experience from this is a mixed one. The Author has had a few meetings with the members of the panel and has received a lot of valuable input to the thesis and metric. At the same time it is demonstrated that the depth of knowledge available to the Author during many months of detailed content analysis and cross referencing makes it very difficult do give real opposition on a possible bias. Considerable more time from the group had been necessary to really "oversee and approve" the results. In this case only the principles presented from the Author was debated.

In the following section "Findings – not related to the research question" we have listed areas of improvement of the analysed documents, which demonstrate the good will to evaluate the work that the Author has been involved in developing.

For the Bank, this may be a topic to address in finalising the metric. For the general reader of this thesis the primary knowledge of interest will be principles and process of designing a metric that can be applied in a different environment. This is addressed in the next section *How to generalize the metric*. Regarding this knowledge there is no reason for expecting a bias.

The risk of proprietary setting

Though this work can result in a useful metric to the Bank, there is a risk that the proprietary setting – from a scientific point of view - may lead to a “home grown *suggestion* of a metric” instead of achieving new general knowledge on metrics that are understood and approved by independent researchers.

To compensate for this possibility we have done the following:

- Cross-referenced with the open security standard SOGP
- Used the Aspects in SOGP to select relevant requirements
- Applied the principles in Frost/Snekkenes, NIST and ISF in an explained process

In addition we have arranged for independent reviews. The Supervisor is the main source for this but we have used Pair review and have sought a second opinion from independent researchers. Their comments have led to several improvements in the report.

One may argue that using SOGP CB as a basis for the metric would lead to a better external validity, a less proprietary metric and lesser resources needed to develop and maintain the metric in the future. This is probably true, but would not have resulted in the metric the Bank needs. The main reason for this is:

- The banks approach to security (See 6.1) focuses more on ease of use and ease of administration then SOGP CB does

- The Security analysis focus more on reusable security solutions then SOGP CB that focus on security requirements – not solutions

8.4 How to generalize the metric

The content of the prototype metric is tailored to the Bank's needs and approach to security, but we believe that others can use the described process of designing the metric to achieve the same goals in a different environment.

The fundament of any metric is the standard to measure against, and we assume that one has defined a security framework for the business (I.e. ISO [1] or SOGP [2]) and the Risk Management concept that security and compliance issues should fit into.

The generic process we recommend based on the knowledge acquired in this thesis is:

- Select the security requirements to be complied with in context of a development project by using the SOGP approach of splitting the framework into Aspects that are relevant to Roles or Stakeholders. Remember Clear line of sight and accountability
- Define the Stakeholders and make sure that one understands their view of the need for and the function of the metric
- Evaluate the Security program maturity to define a realistic type of measurement based on the availability of reliable data
- Evaluate the management and stakeholder support for the metric and define a realistic scope and workload as a starting point
- Define a framework for the metric prototype based on the above
- Define the actual metric content and cross reference it to the requirements to check for validity and reliability
    - Remember "you become what you measure" if one focus on specific issues
- Use Implementation evidence as basis for forming the questions
- Test the prototype metric and improve it with the stakeholders and management
- Decide a process and IT support for the final metric with focus on possible automation of data collection to improve reliability and reduce workload
- Develop and implement the final metric
- Remember that introducing a metric is developing the organisation as your security program matures and the stakeholders learn. The target is constantly moving and the metric must be kept up to date.

The details of each step are described in this report.

This process for designing a security metric is quite similar to what Bakås propose in "Process for measuring the information security level" [34].

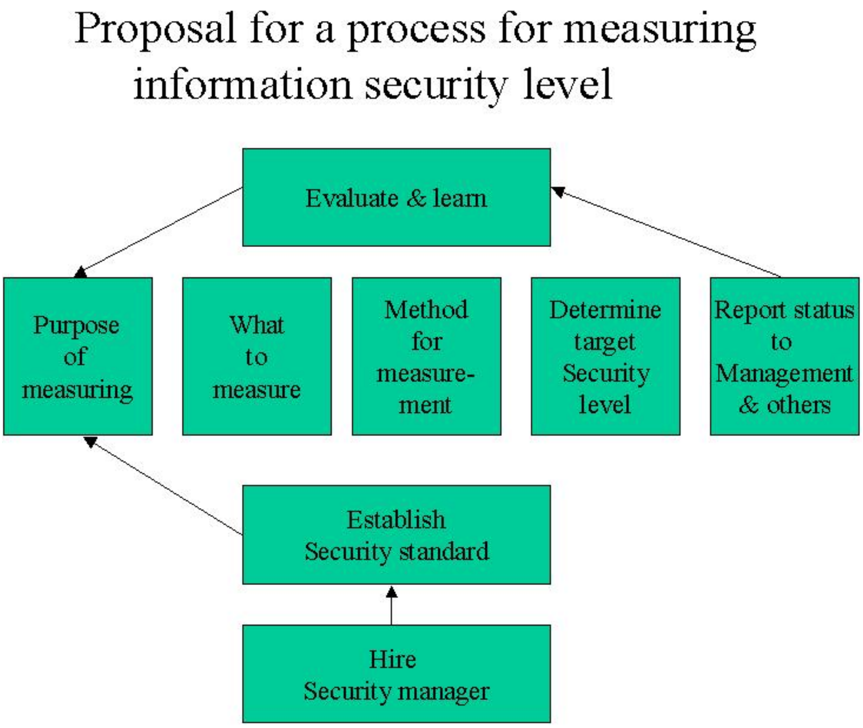

Proposal for a process for measuring information security level
Evaluate & learn
Purpose of measuring
What to measure
Method for measure-ment
Determine target Security level
Report status to Management & others
Establish Security standard
Hire Security manager

Figure 30 A process for measuring [34]

The Authors personal experience

The Author has experience in running security programs and developing metrics and has made some experience that may be of value to others.

The underlying organisational climate decides the way the security metrics will be interpreted and what happens with the measurement and the stakeholder:

- To demonstrate compliance to externals – "telling fairy tails"
- To manage the wild developers - "catch the bad performers red-handed"
- To give stakeholder a feed back to make them learn and improve – "fata morgana"
- To raise the awareness of the security framework – "on the job training"
- To manage risk in the organisation makes good business sense - "Nirvana"

This climate is not a static state and usually there is a combination of all these elements in the organisation. It will vary with factors like maturity, organisational changes, mergers and security specialist dialogue with managers etc.

The person developing a security metric must be well aware of these climate factors.

8.5 Further work

This section has recommendations to the Bank regarding a final Norwegian version of the metric and describes how the Bank can proceed after the MSc thesis:

- Update the Security analysis and the Security metric to the new ITS framework in the Bank and in Norwegian

- Analyse and decide on negative or positive questions regarding compliance both for the Security analysis and for the metric
- Conduct a quantitative Descriptive analysis of a selection of conducted Security analysis from the archive in order to describe security facts and possible consequences related to the systems analysed that can illustrate which topics need to be measured. Examples can be Security analysis' requirements/questions with low compliance rate and high importance, and to describe which security problems the lack of compliance may lead to
- Decide a minimum version of the metric regarding the number of topics to be measured and possible sub-sets for different statistics
- Improve the "Implementation evidence".
  In the prototype we have designed each question or series of questions to test for implementation evidence. We have also tried to give answer alternatives as "algorithm" to set the value of measurement based on implementation facts as described in NIST Sample metrics [4]. This work should be improved as the Bank completes a final Norwegian Metric
- Define and improve the presentation of a Risk profile in a “Spider diagram” and link this presentation of business needs to the area of non compliance and associated risk
- Decide the process for the metric:
  - Stakeholders/Roles and responsibility and use in projects and to management
  - Criterions for accountability for non compliance
- Indicate the most reliable sources for data as described in NIST Metric detail form
  - Source candidates can be parts of test report or security documentation to avoid that the measurement itself becomes the only reliable "security documentation"
- Decide IT support for the Analysis and metric, Excel or a web/db that can automatically:
  - Assist the user in using the process and tool correctly
  - Give easy access to relevant explanations and requirements to understand the context of each question
  - Calculate more complex scores based on the answers (proof of implementation) in a series of related questions
  - Copy data automatically and correct from Security analysis to correct field in Security metric
  - Prepare for automatic data collection from predefined test, macros or sources as indicated in the Security program maturity model from NIST
- Test and retest the same system with different users to ensure reliability.
  - In analysing the measured result, on should use quantitative analysis of the test and retest combined with qualitative analysis to find improvement areas and root cause of errors and bias.
- Develop a final version of the questionnaire for the project's experience with, and perception of, the Security analysis and the associated process.

An assumption is that the introduction of a security measurement at delivery may improve security by itself. The responsible roles will know that their security performance is going to be measured and they know what is being measured.

As a preparation for this thesis, we have discussed the development of secure systems with people with knowledge in the field [20] and the following strategy has been proposed:

- To assist the project in analysing the security issues at project start
- To assist the project in evaluating the security level at delivery by means of a vulnerability review by security specialists (tiger team, red team [10]) or vulnerability scanners

The proposed metric may give some of the answers or serve as a structure for what such a tiger team should test and verify if the Bank decides to use – and staff - such a concept. Tiger teams may have focus on penetrating infrastructure and application to prevent hacking, but the metric can lead to a broader view that includes coherence to standards, robust architecture, elements that improves usability and consolidate security administration.

The metric may also be used for other purposes later:

- It may serve as the basis for a "sign off" document of the actual security status at time of delivery to the business owner
- It may give statistical data (feature vectors) for a regular management report on the overall security performance of the Development division
- It may give statistical data to verify the assumption above:
  that the presence of a metric will increase focus and lead to improved security

8.6 ISF META standard and metrics

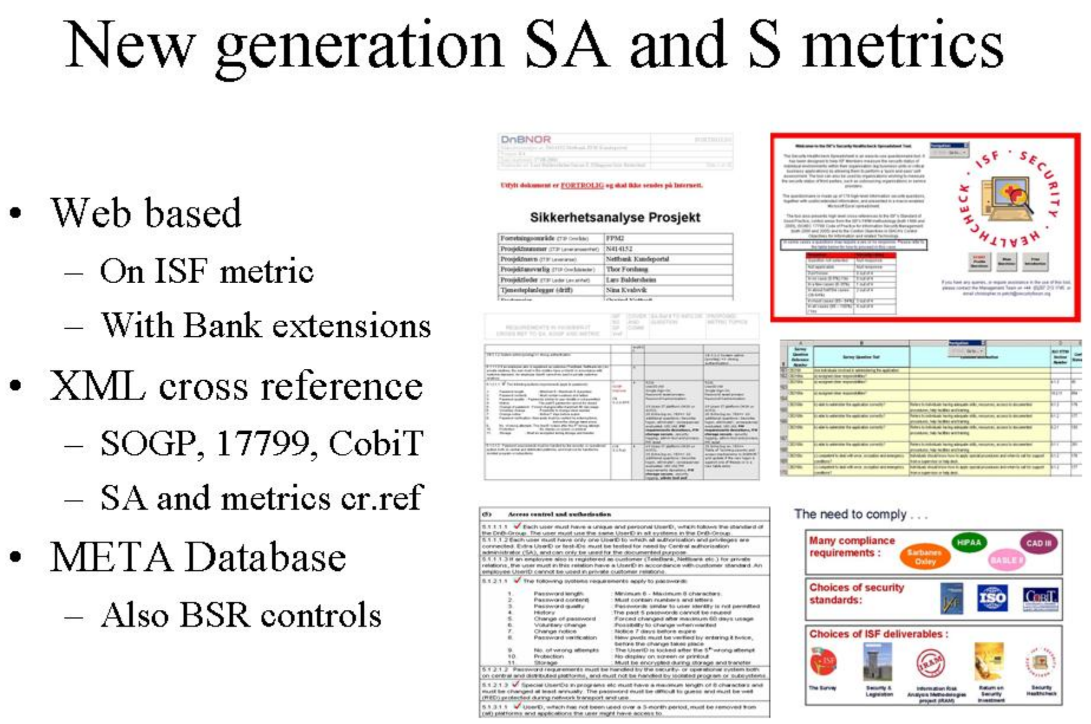
ISF runs a project to propose a Meta standard that ties different standards like ISO 17799 [1], ISF SOGP [2], CobiT [39] and others together in the same database and cross referenced to use the Survey and the Health check to measure compliance against any of them.

ISF is building a new architecture for this based on a 3-layer approach:

- WEB enabled metrics for easy distribution internally in each member organisation
- XML cross reference tables between different metrics and different standards
- A database with all controls from all major standards

We have interviewed ISF management on this issue and propose for the Bank to explore this architecture when deciding IT support for the Security Analysis and the associated Security metric. We have proposed to ISF to open this architecture to its members by adding API's and reserved areas for member extensions, and this has been formally discussed at ISF Council in June.

A possible use for the Bank could be illustrated:



New generation SA and S metrics

- Web based
  - On ISF metric
  - With Bank extensions
- XML cross reference
  - SOGP, 17799, CobiT
  - SA and metrics cr.ref
- META Database
  - Also BSR controls

DnBNOR
Sikkerhetsanalyse Prosjekt
SECURITY HEALTHCHECK
Access control and authorisation
The need to comply . . .
Many compliance requirements :
HIPAA
CAD III
Sarbanes Oxley
BASLE II
Choices of security standards:
ISO
CobiT
Choices of ISF deliverables :
The Survey
Security Healthcheck

Figure 31 New generation of tools

8.7 Findings – not related to the research question

- Improvements or Weak coverage in BSR compared to SOGP BC
- Improvements or Weak coverage in Security analysis compared to BSR and SOGP BC

This will be delivered to the Bank in a separate document due to confidential information.

8.8 Ethical and legal considerations

Relevant literature on security metrics from ISF [2] has been used, and ISF deliverables are only available to members and protected by Copyright. The Bank is a member and is already using different ISF security and risk metrics in several areas.

The Author is a Council member of ISF and has cleared with the Chairman that figures and concepts from the report can be used in a public MSc report as long as it is not making the complete report publicly available and that ISF is properly credited.

The Author has balanced this consideration in his writing and has arranged for a member of ISF Management to read the MSc report.

The complete ISF reports that are referenced can be made available for the supervisor and the sensors to verify that the reports have been referenced and used properly. More information on ISF and how to become a member can be found on the website in [2].

9 Conclusion

We have developed a security metric to measure the security status of an IT system when it is delivered from the development process.

The primary function of the metric is to:

- Document the security status for risk management and compliance purposes
- Measure the effect of the security process and indicate areas of improvement

We have tested and improved a prototype security metric that lays a good foundation for a final Norwegian metric according to the assignment from the Bank. In further work we have described the necessary steps to achieve this final metric. We have also acquired a detailed insight in the Bank's related security documents, which can be used to improve them and the related security process at a later stage.

We have documented the process of designing the metric in a generic form to be used under different conditions and to suit other needs.

This process and metrics framework is built on a combination of scientific principles and industry practice of measuring security, mainly from ISF and the Bank’s own experience.

Examples in this report illustrate how this has been applied to the design of the prototype metric:

- The three step method – why do we need the metric and how does it link to business?
- Defining the stakeholders – who needs the metric and who influence the measured result?
- Clear line of sight and accountability – can the stakeholder see the result of own decisions?
- Security program maturity – is data available and reliable for the planned type of metric?
- Proof of implementation – indicators for degree of compliance?

Measuring security is an immature field and apart from ISF's methods there are not many recognized and wide spread standards for measuring security.

It is hoped that by presenting the knowledge and practical examples in this thesis, it can inspire other to build security metrics in different areas.

Security measurements can demonstrate the business value of reducing risk by investing in security and metrics can assist in maturing the security program by making security visible.

10 References

[1] ISO Standard. 2001. ISO/IEC 17799: Code of practice for information security management.

[2] ISF - Information Security Forum. 2005. The Standard of Good Practice (SOGP) http://www.isfsecuritystandard.com/index_ns.htm (Visited June 2006)

[3] Ingebrigtsen, Deiz and Nilsen. 2004. An evaluation of a practical case of measuring security in an outsourced environment. Gjøvik University College, assignment in course 4111 Security metrics.

[4] Swanson et al. 2003. Security Metrics Guide for Information Technology Systems. Technical Report NIST Special Publication 800-55. (Visited June 2006) http://csrc.nist.gov/publications/nistpubs/index.html

[5] Frost, B. 2000. Measuring Performance – Using new metrics to deploy strategy and improve performance. Measurement International. ISBN 0-9702471-1-7

[6] Payne S. 2001. A guide to security metrics. SANS Security Essentials GSEC Practical Assignment. www.sans.org/rr/papers/5/55.pdf (Visited June 2006)

[7] Wang, C et al. 1997. Towards a framework for security measurement, NISSC, Department of Computer Science, University of Virginia. (From literature list [28])

[8] Bakås, Orderløkken, Hagen. 2003. Sikkerhetsmetrikker for outsourcing av driftstjenester. Gjøvik University College, assignment in course 4111 Security metrics. http://www.hig.no/imt/file.php?id=1042 (Visited June 2006)

[9] Vaughn, Henning, Siraj. 2001. Information Assurance Measures and Metrics. System Sciences, 2003. Proceedings of the 36th Annual Hawaii International Conference, ISBN: 0-7695-1874-5

[10] Wood, B.J., Bouchard, J.F. 2001. Red Team Work Factor as a Security Measurement. Proceedings of the Workshop on Information-Security-System ..., 2001 - philby.ucsd.edu. http://philby.ucsd.edu/~cse291_IDVA/papers/rating-position/Bouchard.pdf. (From [28])

[11] Snekkenes E. 2004. Project description - Security reporting - 06.10.2004. Appliance no ES98333 to Norwegian research council from Gjøvik University College.

[12] Hagen J. 2004. BAS5 - Critical Information Infrastructure Protection. Forsvarets Forskningsinstitutt – FFI. http://www.mil.no/felles/ffi/start/FFI-prosjekter/Alfover/_1014/article.jhtml?articleID=94120 (Visited June 2006)

[13] McHugh J. 2001. Quantitative Measures of Assurance: Prophecy, Process, or Pipedream? CERT/CC 2001. In Workshop on Information Security System Scoring and Ranking, May 2001. http://philby.ucsd.edu/~cse291_IDVA/papers/rating-position/McHugh.pdf (From literature list [28])

[14] McCallam D. 2001. The case against numerical measures for information assurance. http://philby.ucsd.edu/~cse291_IDVA/papers/rating-position/McCallam.pdf (From literature list [28])

[15] Yee, B. S.2001. Security Metrology and the Monty Hall Problem. Workshop on Information Security System Rating and Ranking, ..., 2001 - cs.ucsd.edu. ftp://ftp.cs.ucsd.edu/pub/faculty/bsy/pub/metrology.pdf (Visited June 2006)

[16] KITH. 2004. Indicators for information security/Indikatorer for informasjonssikkerhet. http://www.kith.no/templates/kith_WebPage____727.aspx (Visited June 2006)

[17] Labmice. (No date). Windows 2000 Installation security checklist. http://labmice.techtarget.com/articles/securingwin2000.htm (Visited June 2006)

[18] Leedy, P. 2005. Practical Research, ISBN 0-13-124720-4

[19] Stene, M. 1999. Scientific writing, how to succeed/Vitenskapelig forfatterskap. ISBN 82-463-0025-3

[20] Snekkenes, Einar, Gjøvik University College; Ekelund, Ståle, Accenture, Norway; and Wuchner, Andreas, Novartis International. Personal communication

[21] Creswell J.W. 2003. Research Design: Qualitative, quantitative, and mixed method approaches. SAGE Publications.

[22] Stoddard et al. 2006. Security Metrics Overview. SCADA I3P workshop.

[23] Vaughn, R., Henning, R., Siraj, A. No date. Information Assurance Measures and Metrics - State of Practice and Proposed Taxonomy. In Proceedings of the 36th Annual Hawaii International Conference on System Sciences (HICSS'03) - Track 9 - Volume 9. 2003, IEEE Computer Society.

[24] Henning, R. 2001. Proceedings Workshop on Information-Security-System Rating and Ranking (ISSRR) held in Williamsburg, VA, May 21-23 2001. http://www.acsac.org/measurement/ (Visited June 2006)

[25] Standardiseringsforbund N 1991, Norsk standard: Risikoanalyse NS 5814

[26] Jelen, G. International Systems Security Engineering Association, http://scrc.nist.gov/csspab/june 13-15/jelen.pdf (From literature list [28])

[27] FIPS. 2004. Standards for security Categorisation of federal Information and Information systems. http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf (Visited June 2006).

[28] Snekkenes, E. 2003. A method: How to design a security metric. Lectures from course in Security metrics, IMT5041 at Gjøvik University College.

[29] ISF.2005. Sarbanes-Oxley – implications for Information Security.

[30] AICPA. The Changing Accounting Regulatory Landscape. www.aicpa.org/info/the changing accounting regulatory landscape.htm (Visited June 2006)

[31] AICPA. Summary of Sarbanes-Oxley Act of 2002. www.aicpa.org/info/sarbanes_oxley_summary.htm (Visited June 2006)

[32] Huseby, S. 2003. Innocent code, a security wake up call for web programmers. ISBN 0-470-85744-7

[33] Interview of ISF management:
Jason Creasy: Survey, Health check, Meta std, T 0044 207213 8435
Adrian Davis : Security metrics project and MSc, T 0044 207213 3372
Personal communication

[34] Bakås, T. 2005. Good practice for measuring information security level. MSc report, Gjøvik University College.

[35] Active Directory is Microsoft's repository for users from Windows 2000 and can provide single sign-on to internal applications by Kerberos tickets and to external applications by SAML – Security Assertion Markup Language.
http://search.microsoft.com/results.aspx?mkt=en-GB&setlang=en-GB&q=active+directory
http://support.microsoft.com/?id=555092 (Kerberos)
http://windowssdk.msdn.microsoft.com/en-us/library/8337c432-1b57-4f9d-9a50-87484cd10161.aspx (SAML). (All visited June 2006)

[36] POL – Norwegian abbreviation for Personal data (privacy) act.
http://www.datatilsynet.no/upload/Dokumenter/regelverk/lov_forskrift/lov-20000414-

031-eng.pdf (Visited June 2006)

[37] FPOL – Norwegian abbreviation for "Regulation on the processing of personal data" in relation to POL [36] http://www.datatilsynet.no/upload/Dokumenter/regelverk/lov_forskrift/lov-20000414-031-eng.pdf (Visited June 2006)

[38] ISF. 1995. Organizing security for the 90's. ISF reports library.

[39] ISACA CobiT. (No date). Control Objectives for Information and related Technology. http://www.isaca.org/Template.cfm?Section=Articles1&CONTENTID=22368&TEMPLATE=/ContentManagement/ContentDisplay.cfm (Visited June 2006)

APPENDIX A

Content analysis of the Security Analysis (Only security keywords are used)

CH #	SECTION & PURPOSE	INFO GIVEN TO PROJECT	QUESTIONS TO AND ANSWERS FROM PROJECT	BSR ref
1	**Introduction** To understand Security Analysis	Formal process, roles& responsibility, use of SA	Front of SA: Table of Roles & responsible persons	10.1 17.111
2	**System profile** To understand the business needs, importance and perspective of project	Reference to other documents, laws/acts etc	1 Type of project and 2 Type of system, 3 business functions, 4 and 5 scope of project, 6 security cost covered, 7 “Accounting act”, 8 and 9 “Privacy act”, 10 planned bus. Volume	10.1111
3	**Risk analysis** Business impact only (SPRINT)	Purpose, guide, RA forms for C, I, A	11 Need for RA, existing or new 12 perspective Group or local RA forms for C, I, A	10.3111
3.4	**Security classification** Business need for security controls Mgmnt. approval of risk & class	Requirement and guide	13 Class: Red/High, Blue/Medium, Yellow/Low, or isolated? 14 Mgmnt. approval : Business owner or Steering group	10.3112
4	**Business security requirements** Specify any control of particular importance	Guide with samples	15 Specify any control	10.3112
5	**Selection of security controls, design and solutions**			
5.1	**Security documentation** What to read to understand the proposed security design	Table to reference docs.	16 Reference documents from project	12.2111
5.2	**Access control selection** Type of users and application to	Table: - type of user, # of each type	17 Type of user: Internal, System Adm, Superuser, Customer care/adm, External user/customer, Agents,	

CH #	SECTION & PURPOSE	INFO GIVEN TO PROJECT	QUESTIONS TO AND ANSWERS FROM PROJECT	BSR ref
	jump to relevant section in SA	- in which part of the system	Admin at external site	
	Select one or two-factor authentication, reduced sign on, avoid external exposure of internal functions	Illustration fig. Table: - type of application environment	18 Type of application environment: Internal appl. for internal users, Web for internal, Web for external, External appl. for internal, Web for customers, Web for Agents, Common web application for internal & customer, other	
5.2.2	Internal application for internal users			
5221	Authentication and Identity mgmnt	UserID std Single Sign-On Password reset process Password harmonisation	19 User IT platform (W2K or ACF2) 20 Extra log on, YES=> 10 additional questions Describe logon, eliminate?, consequences evaluated, UID std & PW requirements deviation, PW storage secure, security logging, admin tool and process, PW reset	5.1 5.2 5.4 6 6.5
5222	Authorisation, Access control, Access mgmnt	Preferred sec. systems Design model Avoid internal tables Sec.Adm.Mgr SAM Business Access roles Admin process Describe in standard Formulary Internal access to e-applications via internal DMZ (not external)	21 Internal solutions/tables 22 Describe access solution 23 use of SAM and Business access roles 24 Avoid external exposure of internal functions	5.3 5.4
5.2.3	Web appl. for external users/ customers			
5231	Authentication and Identity mgmnt	UserID std Strong 2 factor authentication	25 Portal, 26 Authentication SR, 27 URL-jump to external site, 28 Deviations from e-architecture	

CH #	SECTION & PURPOSE	INFO GIVEN TO PROJECT	QUESTIONS TO AND ANSWERS FROM PROJECT	BSR ref
		Single Sign-On from portal		
5232	Authorisation, Access control, Access mgmnt	Preferred sec. system TAM Design model Avoid internal tables	29 Internal tables, 30 SR Admin, 31 Customer internal admin, 32 Describe how internal functions and external (customer) functions are kept separated	81323
5.2.4	External system for internal users	Do NOT reuse internal UID /PW SSO with ticket or URL Jump	33 Describe 8 topics: Authentication, Authorisation (Access), Administration tool, security logging, Administration process for Identity, access and passwords, access reporting to management.	51313
5.3	**Authentication, Authorisation and Access control for programs**	Recommended solution: - run as privileged service - access via program UID Must be registered in SLA for "Non personal UID"	34 Privileged service approved by responsible 35 Program UID via request process and SLA	5212, 51313
5.4	**Securing application data**	Avoid SQL direct against DB and avoid that users are given access direct to DB – give access to appl instead	36 Direct user access to application data 37 Sensitive data (POL) ? 38 New crypto keys or systems register in SLA	12.3112 7.1 7.2
5.5	**Network and data exchange**			
5.5.1	Description and analysis (Communication profile)	All external connections must pass the Firewall regime and respect trust zones	39 Network sketch, 40 System components and thrust zones, 41 Identify networks, 42 External communication	
5.5.2	Data exchange	Defines trusted path and trusted channel Explains where Authentication, encryption and integrity protection is needed Preferred security products	43 Data content, 44 Protocol, 45 DMZ-> direct to internal? 46 Authentication, 47 External communications? Password exch. or security transactions 48 Confidentiality, 49 Integrity, 50 New crypto keys or systems register in SLA	51213 7.1

CH #	SECTION & PURPOSE	INFO GIVEN TO PROJECT	QUESTIONS TO AND ANSWERS FROM PROJECT	BSR ref
		(Ex Connect Direct) FW change request process	51 Change in Firewall needed?	
5.5.3	Authentication and Authorisation of systems exchanging data	See also 5.3	52 Program UID via request process and SLA	51213 9.2
5.6	**Secure code and security testing**	Principles for secure code and code review System penetration against application and infrastructure	53 Secure code and security testing 54 Input validation 55 Application IDS/Anomaly	11.1113 67112
5.7	**Audit, logs and Incident handling**	Audit trail and SETA for business transactions	56 Business log 57 IDS sensors 58 IRT Info	6 67112 67113
5.8	**Technical platform and IT operations**	Reference: The banks Standards & Products	59 Deviation from Standards & Products platforms, 60 Databases, 61 Freeware/shareware, 62 Active content (ActiveX, Script ++)	11.1114 12.1113 17.111
5.9	**Resilience, business contingency**	Standard levels for disaster recovery Testing security	63 Alternative site, backup, capacity, recovery time 64 Single point of failure	81343 14 15
5.10	**System maintenance, operation and SLA**	Roles and responsibility Service provider represented by Service planner (TPL)	65 Security remarks from external Service provider 66 Maintenance agreement, SLA 67 Remote Maintenance or Operation	11.1114 12.1113 12.3113
5.11	**Transaction system**	Relates to 5.2.2 United Time Code UTC for synchronised clocks 2 independent logs A coherent log chain as evidence	68 Batch or store and forward 69 Financial transaction requires integrity protection/digital signature 70 Synchronised clocks for logging 71 Coherent log chain	 71212 62411 63111
6	**Risk summary**	Be aware that SA does not cover	72 Deviations from security framework and risk	10.3111

CH #	SECTION & PURPOSE	INFO GIVEN TO PROJECT	QUESTIONS TO AND ANSWERS FROM PROJECT	BSR ref
		all possible scenarios and parts of the security framework	73 Other security factors that may pose risk 74 Overall risk assessment	10.3112 12.1113
7	**Measures to reduce risk**	“The most important results from SA is action”	75 Describe planned measures and risk reduction	10.3111

The Metric build on the following assumption:

Metric is building on the structure of Security Analysis to make comparison simple and re-use data from SA whenever possible
Section 1-5 is mainly copy from SA content analysis

Some structure change has been conducted and will influence next version of SA. (order of topics in chapters and illogical splits of topics)

Metric wording should generally not repeat BSR but this test version will use BSR wording for clarity. A planned web-based solution that combines the SA with the metric may link to the relevant BSR requirements with exact wording.

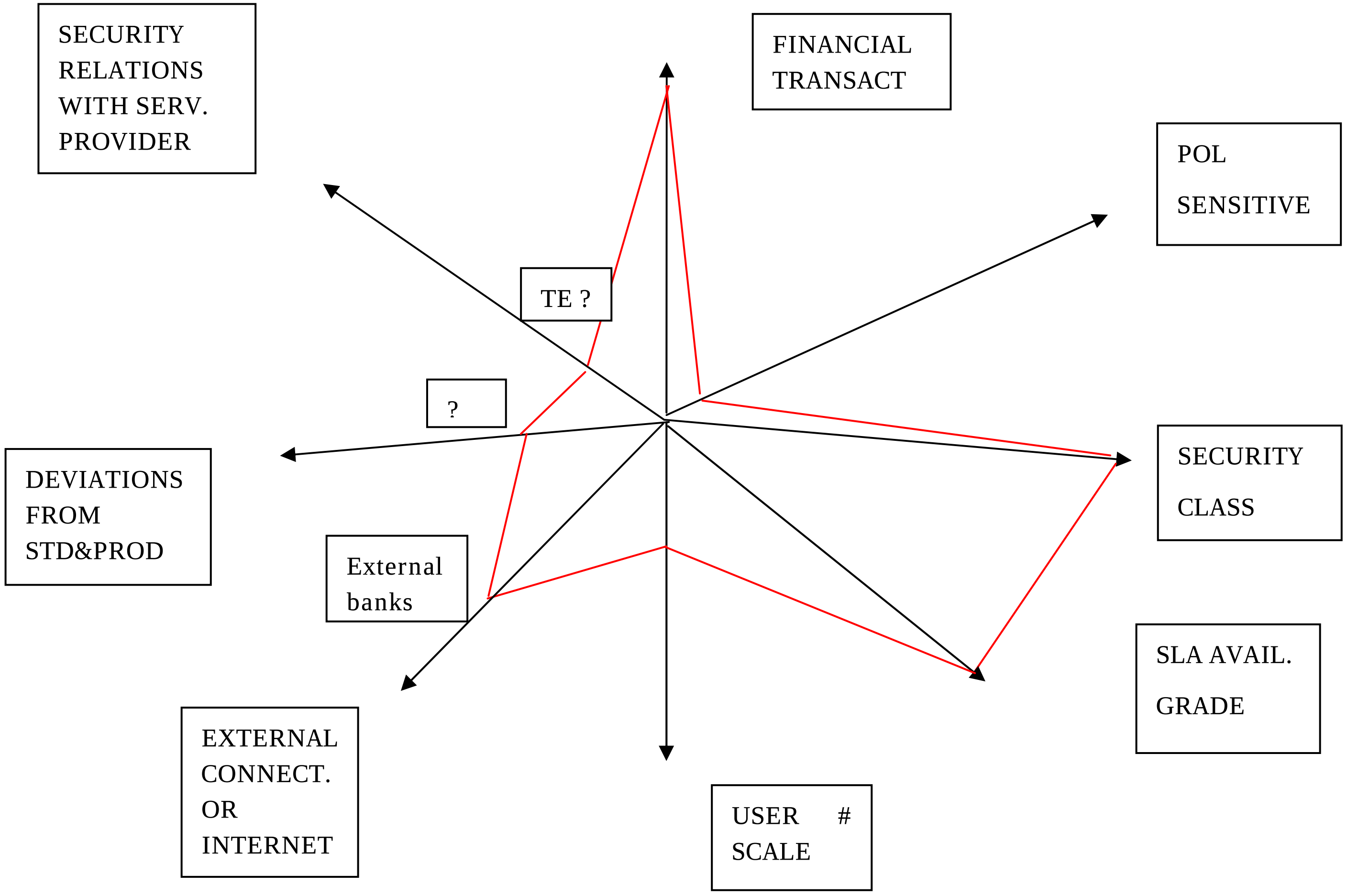
Metric will give full credit for recommended reusable security solutions even if the solution has known weakness.
(Evaluation of recommended solutions – ex SAM - should be done separately by SA and using the metric on such solutions)

For Further work:

Each question should have a comment field for reason of lower score than max. Areas of lower score than 3 + these comments should be presented for risk management purpose

Roles & responsibility must be explained, particularly the responsibility of the service planner from service provider

Can / should the metric be an integrated part of the security documentation and test plan for the system?



RISK FACTORS FROM SYSTEM PROFILE Sample

SECTION, PURPOSE & INFO **NEW METRICS**	**ANSWER ALT. TO METRIC**	**INFO FROM SA + METRIC ANSWERS**

START OF INTRO AND SYSTEM INFO		
1. Introduction To understand Security Analysis		
Chapter 1 Introduction: Formal process, responsibility, use of Security Metric Table of Roles and responsible person for the complete system		
2. System profile To understand the business needs, importance , perspective and legal limits Reference to other documents		
1 Type of project		
2 Type of system		
3 business functions		
4 / 5 Scope of project and security analysis		
6 Is security cost covered		
7 Is “accounting act” (Regnskapsloven) relevant		
8 Is “privacy act” (POL) relevant		
9 POL countermeasures if sensitive		
10 Planned bus. Volume		
Will the SLA have an A grade in requirements level or are there		

SECTION, PURPOSE & INFO **NEW METRICS**	**ANSWER** **ALT. TO** **METRIC**	**INFO FROM SA + METRIC ANSWERS**
other indicators of Critical Business Application/process?		
See also security classification CIA		
Bank risk table input		
Control selections in IRAM: External connections External users/3.party web/Internet/Wlan/BT Portable or new device Infrastructure?		
3. Risk analysis Business impact only (SPRINT) Purpose, guide, RA forms for C, I, A		
11 Need for RA, existing or new RA forms for C, I, A Recent Risk Analysis of complete system? New RA of complete system required?		
12 perspective Group or local		
3.4 Security classification Business need for security controls Mgmnt Approval of risk & class Requirement and guide		
13 Class: Red/High, Blue/Medium, Yellow/Low, or isolated? New exposure of total system?		

SECTION, PURPOSE & INFO **NEW METRICS**	**ANSWER** **ALT. TO** **METRIC**	**INFO FROM SA + METRIC ANSWERS**

Review or confirm class		
14 Mgmnt Approval : Business owner or Steering group		
4. Business security requirements Specify any control of particular importance Guide with samples		
15 Specify any control of particular importance to bus.		
5. Selection of security controls, design and solutions Select solutions for external or internal needs: one or two-factor authentication, reduced sign on, avoid external exposure of internal functions		
5.1 Security documentation What to read to understand the proposed security design Table to reference docs.		
16 Reference documents from project (Is covered in ch 5.10, 65.10)		
5.2 Access control selection Type of users and application to jump to relevant section in SA		
Table: - type of user, # of each type - in which part of the system		
17 Type of user: Internal, System Adm, Superuser, Customer care/adm, External user/customer, Agents, Admin at external site		
Illustration fig. Table: type of application environment 18 Type of application environment: Internal appl. for internal		

SECTION, PURPOSE & INFO NEW METRICS	ANSWER ALT. TO METRIC	INFO FROM SA + METRIC ANSWERS

users, Web for internal, Web for external, External appl. for internal, Web for customers, Web for Agents, Common web application for internal & customer, other		
END OF SYSTEM PROFILE - METRIC STARTS		
5.2.2 Internal appl. for internal users		
5.2.2.1 Authentication and Identity mgmnt UserID std, Single Sign-On Password reset process Password harmonisation		

19 Which IT platform are the users workstation connected to?
IF "OTHER" PLATFORM:
The whole 522 section must be run to test the security of the user platform
	W2k =4
	
	ACF2=3	

20 Is SSO used to avoid external logon (except against 3270)?
YES=>
Which SSO is used:
a win 2k Kerberos
b win 2k ACF2 ticket
a1 In-house (Tr)
b1 Security Object
c1 Other
	
	Y=4
	Y=4
	Y=1
	Y=2
	0-4	

(NO => Extra logon required)
20. 01 Chose from Table of "existing security and access mechanisms in the Bank" or update if the new logon is a new table entry
20.02 existing or new access mechanisms?
	Existing=1
	New =0	

20.1Is logon a part of a Cots operating system or a programmed	Cots=4	

SECTION, PURPOSE & INFO **NEW METRICS**	**ANSWER ALT. TO METRIC**	**INFO FROM SA + METRIC ANSWERS**
part of the system		
20.2 Is elimination planned?	Y=4	
20.3 Are consequences documented and accepted by business mgmnt	Y=4	
20.4 Are there UID std & PW requirements deviation	No=4	
20.5 Are password stored securely and one way encrypted	Y=4	
20.6 Are passwords encrypted in transmission	Y=4	
20.7 Any deviations from security logging regarding the extra logon (See 5.7)	No=4 0-3	
20.8 Are SAM and Admin process used for administering users? NO 20.8a Is the administration process described and tool tested	Y=4 0-3	
20.9 Deviation from standard PW reset process?	N=4	
YES 20.91 Are passwords reset in a secure process (ref CB 3.1.4) 20.92 Are 1. password and reset pw **not** easily guessable?	Y=4	
20.10 Warning of hacking in logon screen?	Y = 4	
20.11 Is a message about date and time for the last log on, and number of failed attempts since the last successful log on displayed?	0-4	
20.12 Deviation from pause/PW lock function?	0-4	
20.13 Is a method of ensuring that users do not share UID/PW implemented? (Ex "Already logged on")	0-4	
20.14 Is sign on re- invoked after a connection is broken?	Y=4	
5222. Authorisation, Access control, Access mgmnt Preferred sec. systems Design model	16	

SECTION, PURPOSE & INFO **NEW METRICS**	**ANSWER ALT. TO METRIC**	**INFO FROM SA + METRIC ANSWERS**
Avoid internal tables Sec.Adm.Mgr SAM Business Access roles Admin process Describe in standard form Internal access to e-applications via internal DMZ (not external)		

21 Is access controlled only by W2K, ACF2 or?
NO
21.1 Is access controlled by Cots operating system (and not a programmed part of the system by internal access tables)?
NO
Chose from Table of "existing security and access mechanisms " or update if the new logon is against one of these or is a new table entry
21.2 existing or new access mechanism
	Yes=4
	No but existing=1
	SAM: Mail via Gen TSI =2
	New =0	

23 Is access administered through SAM? 23.1 Is SAM mail from TSI used 23.2 Is the user access incorporated into existing business roles or is only new function roles created?	Yes =3 SAM mail=2 Existing roles =1 SUM?	
23.3 Is access administration process integrated with existing or new/separate?	Existing LA=4	
(NEW /separate) 23.4 Are list of users and their access (roles) sent to responsible managers in the bank?		

SECTION, PURPOSE & INFO **NEW METRICS**	**ANSWER ALT. TO METRIC**	**INFO FROM SA + METRIC ANSWERS**
23.5 Are dormant accounts removed from the system?		

23.11 Any users in the system will have Privileges ('Admin')?
Is Principle of least privilege followed
Are privileges visible in SAM?
	No =4
	Yes =1
	Yes=2
	Sum=	

23.12 Are any (end) user given direct access to:
- Application data?
- Production environment (program, parms, files, scripts)?
	No=4
	Yes =0	

24 Are internal function of the system only available via internal Network (or internal DMZ) or are they also accessible from external network connections (ex Internet or mobile access) If no – is this Tested?	Tested No=4 Yes = 0	
	22+16=38	
5.2.3 Web appl. for external users/ customers		
5231. Authentication and Identity mgmnt UserID std Strong 2 factor authentication Single Sign-On from portal Policy for URL-jump to external site		
25 Do external users logon to a standard portal according to e-framework with no deviations? Which portal?	Yes=4	
Table of Auth-methods 26 Do external users use a strong authentication from SR	Yes = 4	
27 Is user redirected to external site via URL-jump	No=4	

SECTION, PURPOSE & INFO **NEW METRICS**	**ANSWER ALT. TO METRIC**	**INFO FROM SA + METRIC ANSWERS**
Deviations from URL-jump policy?		
28 has the application any deviations from e-architecture, standards or security concepts	No=4	
5232. Authorisation, Access control, Access mgmnt Preferred sec. system TAM Design model Avoid internal tables	38+4=42	

29 Are internal tables avoided (using TAM and SR Admin)
NO
Chose from Table of “existing security and access mechanisms” or update a new table entry
29.1 existing or new access mechanism
	Yes =4
	Existing=2	

30 Is SR-admin used?	Y=4	
31 Is customer user administration delegated to customer as standard	Yes=4	
32 Are any internal function of the system available from external network connections (ex Internet or mobile access) 32.1 Can internal functions by accident be granted to external (customer) or are they only available through internal DMZ? Tested?	No+No=4	
	42+4=46	
5.2.4 External system for internal users Do NOT reuse internal UID /PW SSO with (SAML), ticket or URL Jump		
33 Is SSO used to avoid external logon? YES - is SSO with SAML used?	SSO by SAML=4	

SECTION, PURPOSE & INFO **NEW METRICS**	**ANSWER ALT. TO METRIC**	**INFO FROM SA + METRIC ANSWERS**

- else		
(NO => Extra logon required) 33.1 Is Service Provider in a security contract relation with us so we can thrust them internal UID and PW? YES > use UID + PW	Yes=4	

(NO=> Separate UID and PW must be used)
33.11 are internal UID and PW prohibited automatically
33.12 Are UID uniquely related to individual
33.13 Are PW of sufficient quality
33.14 Are PW stored securely and one way encrypted
33.15 Are PW encrypted in transmission
	Yes=4
	Yes =4
	
	Yes=4
	Yes=4	

21 Is access controlled by a Cots operating system (and not a programmed part of the system by internal access tables)? NO Chose from Table of "existing security and access mechanisms " or update if the new logon is against one of these or is a new table entry 21.1 existing or new access mechanism	Yes=4	
33.15 Is access administered through SAM and SAML or through SAM and generic TOM with mail to external administrator? YES 33.16 Is the user access incorporated into existing business roles or is only new function roles created? 33.17 Are inconsistence between external register and SAM	Yes=4 SAM Mail=2	

SECTION, PURPOSE & INFO **NEW METRICS**	**ANSWER ALT. TO METRIC**	**INFO FROM SA + METRIC ANSWERS**

resolved?		

33.18 Is access administration process integrated with existing or new/separate	Existing=4
	New=2	

33.19 Are list of users and their access (roles) sent to responsible managers in the bank? 33.20 Are dormant accounts removed from the system?		
33.21 Are passwords reset in a secure process (ref CB 3.1.4) 33.22 Are 1. password and reset pw **not** easily guessable?	Yes=4	
5.3 Authentication, Authorisation and Access control for programs Recommended solution: - run as privileged service - access via program UID Must be registered in SLA for “Non personal UID”	46+8=54	

34 Are privileged programs and TCB modifications needed
YES
Are privileged programs and TCB modifications:
- registered
- risk evaluated
- approved by responsible
	No=4
	
	YYY=3	

35 If program UID needed: Are they acquired via request process and SLA? Describe how many and context for use	Yes=4	
35.2 Is password to IPB protected		

SECTION, PURPOSE & INFO **NEW METRICS**	**ANSWER ALT. TO METRIC**	**INFO FROM SA + METRIC ANSWERS**

35.3 Is Audit requirement of real users UID needed and fulfilled	Yes =4	
	54+2=56	
5.4 Securing application data Avoid SQL direct against DB and avoid that users are given access direct to DB – give access to application instead		
(See 23.12) 36 Direct user access to application data	NO=4	
37 Is anything encrypted on storage?	Y=4	

YES
38 Are new crypto keys registered in SLA?
38.1 Is a new crypto system introduced?
YES
Is the new crypto system approved by ITS?
	Y=4
	
	Y+
	Approved=4	

38.2 Has data /functions been moved to a less secure "environment"	No=4	
	56+4=60	
5.5 Network and data exchange		
5.5.1 Description and analysis (Communication profile) All external connections must pass the Firewall regime and respect of trust zones		
39 Network sketch		
40 System components and thrust zones		
41 Identify networks		
42 External communication 42 versus 47??		
	60	

SECTION, PURPOSE & INFO **NEW METRICS**	**ANSWER ALT. TO METRIC**	**INFO FROM SA + METRIC ANSWERS**
5.5.2 Data exchange Defines trusted path and trusted channel Explains where Authentication, encryption and integrity protection is needed Preferred secure data exchange products (Ex Connect Direct – NOT FTP) FW change request process		
44 Is used protocol a “new” protocol to the bank Any known security weakness in used protocols	N0=4 Yes but countermeasure=2	
45 Any deviations from network security concept? - DMZ-> direct to internal - New external connections not through FW	No=4	

46 Is chosen data exchange product giving authentication?
46.1 authentication 2 way or in the direction important for us?
	Yes=4
	Yes=2	

47 does the system have any **new** external connections – included portable or device: - Wifi, BT, Infra, modem	No=4	
48 Are any data encrypted in external transmission? 48.1 Are any passwords, keys, security transactions sent unencrypted	Yes+ No=4	
49 (69) Are any Financial transactions sent without integrity protection/ digital signature (Non repudiation) 49.1 (68) Batch or store and forward	No =4	

SECTION, PURPOSE & INFO **NEW METRICS**	**ANSWER ALT. TO METRIC**	**INFO FROM SA + METRIC ANSWERS**

50 IF new Keys- Are new crypto keys registered in SLA?
5.11 Is a new crypto system introduced?
YES
Is the new crypto system approved by ITS?
	Y=4
	
	Y+
	Approved=4	

51 Change in Firewall needed? Yes: FW rules with least access/privilege?	Yes+Yes=4	
	60+9=69	
5.5.3 Authentication and Authorisation of systems exchanging data		
52 Program UID via request process and SLA See also 5.3		
5.6 Secure code and security testing Principles for secure code and code review System penetration against application and infrastructure		
53.1 Is the code reviewed for security flaws (ref Innocent code)? - by agreed expert - by “second opinion”	Yes, by agreed expert =4	
53.2 Are all input from user validated against misuse by white list/filtering on content, meta characters and valid size of input? (ref Innocent code)	Y=4	
53.3 Is penetration conducted? - by primary Service provider or other/in-house - to infrastructure - to application	Yes, to both Infra and appl.=4	
53.3 Are all security functions in this metric tested? Is the system negative tested Are existing security controls tested for effects of the change?	Y=4	

SECTION, PURPOSE & INFO NEW METRICS	ANSWER ALT. TO METRIC	INFO FROM SA + METRIC ANSWERS
55 Are any countermeasure built in aimed at detecting or preventing anomaly or attacks at application level? See 57	Y=4	
	69+5=74	
5.7 Audit, logs and Incident handling Relates to 5.2.2 United Time Code UTC for synchronised clocks 2 independent logs A coherent log chain as evidence		
56 Is SETA used for business transactions or a similar common business log?	Y=4	
56.1 Are any functions not leaving trace/log (6.2.2.1.3)	N=4	
70 Are clocks for logging synchronised with deviations > 2 seconds from time Norwegian std time with NTP/UTC or similar?	NTP/UTC=4	
71 Is a consistent log chain between Bus.log <> sec.log tested? Is a desk-test of “false transaction complaint” with use of logs performed?	Desk test performed =4	
71.1 Are there two independent logs in the chain? (Independent means that collusion is necessary to forge both logs identical)	Y=4	
71.2 Deviations from bus and sec log record std content 62112, successes 65111 or violations 65112?	No=4	
71.3 Is log data on line > month, easily available, and kept for min 13 months	Y=4	
71.4 Are controls of logs conducted to prevent and discover unauthorised access?	Y=4	
57 IDS sensors	Y=4	

SECTION, PURPOSE & INFO **NEW METRICS**	**ANSWER ALT. TO METRIC**	**INFO FROM SA + METRIC ANSWERS**
Are HIDS / NIDS sensors giving the application adequate protection?		
58 IRT Info Is Info and Reporting of errors and security incidents described and agreed with IRT in the Bank Is vendor’s IRT operational regarding this system?	Y=4	
58.1 Agreed with IRT how logs can be consolidated?	Y=4	
	74+11=85	
5.8 Resilience, business contingency (SA 5.9) Standard levels for resilience and disaster recovery Testing		
63 Alternative site, backup, capacity, recovery time 63.1 Are arrangements completed and documented to meet the levels in 63? 63.2 Has restore been tested 63.3 Is the system covered by a business contingency plan in case of unavailability of SW, Info/Data, Network, key staff, buildings/data room, access to...in crises 63.4 Is the contingency plan tested?	Yes=4 Yes=4 Yes and tested=4	
64 Has a Single point of failure analysis been conducted Has technical resilience measures have been implemented (ex: fault tolerance, 2 hot sites, transaction recovery, Mirror/RAID,	SPF conducted and	

SECTION, PURPOSE & INFO NEW METRICS	ANSWER ALT. TO METRIC	INFO FROM SA + METRIC ANSWERS

dedicated hw, dedicated NW/Zone, comm. partners screened, UPS)	reasonable resilience in proportion to risk profile=4	
	85+5=90	
5.9 Technical platform and IT infrastructure (SA 5.8 + operations)		

59+60 Deviation from Standards & Products (Platforms, Databases, middleware etc)
Is the deviation approved by "Infrastrukturforum"
	No=4
	Yes=2	

61 Any Freeware/ shareware	No =4	
62 Any Active content (ActiveX, Script ++)	No=4	
	90+5=95	
5.10 System maintenance, IT operation and SLA Roles and responsibility Service provider represented by Service planner (TPL)		
65 Security remarks from external Service provider (via Service planner)	N0=4	
65.1 Is the system operation outsourced to another Provider then main (SP1)?	No=4	
IF YES: 65.2 Is there an agreement with a standard IT security appendix (ref bilag 8) 65.3Is the agreed security performance reported and controlled 2 times a year 65.4 Are the Providers people appointed to the relevant roles in	Y=4 Y=4	

SECTION, PURPOSE & INFO **NEW METRICS**	**ANSWER ALT. TO METRIC**	**INFO FROM SA + METRIC ANSWERS**
writing 65.5Are the roles quality assuring the measurements in this metric? 65.6 Are the Service planner contributing to security on behalf of Provider	Y=4 Y=4 Y=4	
(See also 5.1 Sec Documents – move 5.1 here? check for exist or read for understand problems relevant to metrics answers)		
65. 10 Is IT operation documentation written including IT Security documentation (Check answer to 22 Describe access solution in std document)	Y=4	
65.11 Has security functions been tested according to this metric and checklist in Test directory? (See 53.3)	Y=4	

66.1 Has an maintenance agreement been entered
66.2 Has an SLA been entered?
66.3 What is the requirements level (A..) in SLA
	Y=4
	Y=4
	A=0 B=1	

67 Has the application Remote Maintenance or Operation?
67.1 Has business accepted the risk of Remote Maintenance or Operation
67.2 Is access solution described in 5.5.2 and approved by Network security
	N=4
	Y=4
	Y=4	

(New external connections and business relations must be covered by a Third Party agreement)		
67.10 Does the system introduce any new external connections or business relations (Ex external business partners, customers, Remote Maintenance or Operation, delivering Service to external users)	N=4	

SECTION, PURPOSE & INFO **NEW METRICS**	**ANSWER ALT. TO METRIC**	**INFO FROM SA + METRIC ANSWERS**

YES 67.11 Are Third Party agreements covering the different parties entered? 67.12 Does the agreement clarify -security responsibility and duties that rest with each partner? - how these duties and responsibilities will be controlled or tested?	Y=4 Y=4	
67.20 Is Development, Test and Production separated securely Has any developer write-access to production Has all test aids like trace, backdoors, short cuts been removed	Y=4	
(New: Physical security of Data installations)		

67.30 Anything situated outside secure Data rooms in Service provider?
67.31 Anything situated outside secure Data rooms in the bank?
	N=4
	N=2	

	95+19=114	
(New: Insurance)		
67.40 Has the need for insurance been evaluated Ex. Interruption of Critical business Systems or damage to hardware? 67.41 Has the need for warning to insurers been evaluated on changes of risk from business process or system (ex LLOYDS Data crime: acquisition and mergers with banks or delivering of new services to other banks)	Y=4 Y=4	
	114+2=116	
6. Risk summary Be aware that SA does not cover all possible scenarios and parts		

SECTION, PURPOSE & INFO **NEW METRICS**	**ANSWER ALT. TO METRIC**	**INFO FROM SA + METRIC ANSWERS**

of the security framework		
72 Deviations from security framework and risk		
73 Other security factors that may pose risk		
74 Overall risk assessment		
7. Measures to reduce risk "The most important results from SA and Metric is action"		
75 Describe planned measures and risk reduction		