DEGREE PROJECT IN COMPUTER SCIENCE AND COMPUTER ENGINEERING,
SECOND LEVEL
STOCKHOLM, SWEDEN 2016

Security Management

Fulfillment of the Government Requirements for a component assurance process

NAIDA KUKURUZOVIC

KTH ROYAL INSTITUTE OF TECHNOLOGY
INFORMATION AND COMMUNICATION TECHNOLOGY

Security Management

Fulfillment of the Government Requirements for a component assurance process

Naida Kukuruzovic

2016-07-26

Master's Thesis

Examiner
Gerald Q. Maguire Jr.

Supervisor
Anders Västberg

Industrial adviser
Admir Muhovic

KTH Royal Institute of Technology
School of Information and Communication Technology (ICT)
Department of Communication Systems
SE-100 44 Stockholm, Sweden

Abstract

Protecting organization's assets from various security threats is a necessity for every organization. Efficient security management is vital to effectively protect the organization's assets. However, the process of implementing efficient security management is complex and needs to address many requirements.

The problem that this master's thesis project addressed was to propose a component assurance process for the Swedish Armed Forces. This process has to be followed in order for a solution or product to be approved at a specific component assurance level. This problem was solved by first performing market research regarding security management. Various security management approaches were examined and the top security management solutions were selected. These solutions were then compared with the assurance requirements stated in Swedish Armed Forces' KSF v3.1 (Swedish: "Krav på IT-säkerhetsförmågor hos IT-system", English: Requirements for IT security capabilities of IT systems). This documentation lists the requirements for information technology (IT) security capabilities of IT systems. The solution that satisfied the most of these requirements was selected and modified in order to satisfy the full set of requirements. Finally, a component assurance process is proposed. This process may be used to decide which solutions or products can be used, along with the manner in which each solution or product should be used. The impact of having a component assurance process is that all the solutions and products are approved to a specific component assurance level exclusively based on this process. The ability to include such requirements in the acquisition of any product or service provides the Swedish Armed Forces with assurance that all products or services are approved to specific assurance levels in the same manner and hence provides the Swedish society with assurance that procedures within the Swedish Armed Forces are documented and protect the interests of the country and its citizens.

Keywords

Security management, information security, authentication, authorization, governance, risk management, compliance, user management

Sammanfattning

För varje organisation är det nödvändigt att skydda information från olika säkerhetshot. Att ha en effektiv säkerhetshantering är avgörande för att kunna skydda informationen. Denna process är komplex och många krav måste tillfredsställas.

Problemet som detta examensarbete avser att lösa handlar om hur införandet av en assuransprocess kommer påverka Försvarsmakten. Denna process måste följas för att en lösning eller produkt ska godkännas till en specifik komponents säkerhetsnivå. Frågeställningen besvaras i första hand av en marknadsundersökning om säkerhetshantering. Olika säkerhetshanteringsstrategier undersöktes och de bästa säkerhetslösningar valdes. Lösningarna jämfördes därefter med de assuranskrav som anges i Försvarsmaktens KSF V3.1 (Krav på IT säkerhetsförmågor hos IT – system) som är den dokumentation som anger kraven för IT säkerhetsfunktioner i ett IT system. Lösningen som uppfyllde de flesta kraven valdes och modifierades för att uppfylla samtliga kraven. Slutligen rekommenderades en komponent assuransprocess, vilken skulle kunna användas för att avgöra vilken lösning eller produkt som skulle kunna användas samt på vilket sätt det skulle kunna användas. Möjligheten att införa sådana krav i förvärvet av vilken produkt eller tjänst det än gäller förser Försvarsmakten med garantier för att alla produkter eller tjänster är godkända enligt särskilda säkringsnivåer på samma sätt och därmed försäkras det svenska samhället att förfaranden inom svenska väpnade krafter dokumenteras samt skyddar landet och dess medborgare.

Nyckelord

Säkerhetshantering, informationssäkerhet, autentisering, auktorisering, styrning, riskhantering, följsamhet, användaradministration

Acknowledgments

This master's thesis project exists thanks to the help, encouragement and inspiration from several people, namely:

Professor Gerald Q. Maguire Jr., for his continuous support, valuable feedback, and constructive criticism.

Professor Anders Västberg, for being my supervisor.

Admir Muhovic, for giving me an opportunity to work on this project.

Jasmir Beciragic, for his advice and infinite support.

Mia and Mirza, for all the received encouragement.

My greatest gratitude goes to my parents and brother, for the unconditional support throughout my studies and life.

Stockholm, July 2016
Naida Kukuruzovic

Table of contents

List of Figures

List of Tables

List of acronyms and abbreviations

CA	Certificate Authority
CM	Configuration Management
COBIT	Control Objectives for Information and Related Technology
DDoS	Distributed Denial of Service
DoS	Denial of Service
GRC	Governance, Risk Management, and Compliance
HIDS	Host Intrusion Detection System
HIPS	Host Intrusion Protection System
IAM	Identity and Access Management
IGA	Identity Governance and Administration
ISMS	Information Security Management System
IT	Information Technology
ITIL	IT Infrastructure Library
ITSS	IT System Security Specification
NAC	Network Access Control
NIDS	Network Intrusion Detection System
NIPS	Network Intrusion Protection System
OECD	Organization for Economic Co-operation and Development
OS	Operating System
PDI DSS	Payment Card Industry Data Security Standards
PIN	Personal Identification Number
PKI	Public Key Infrastructure
SIEM	Security Information and Event Management
S-TAP	Software-Tape
UNESCO	United Nations Educational, Scientific, and Cultural Organization

1 Introduction

Today many security risks and threats could cause harm to organizations' assets. Organizations such as the military require the highest level of protection due to the sensitivity of the information that is being stored and manipulated in their Information Technology (IT) systems. Unauthorized disclosure of such information might lead to harm to both the organization and society. Security management procedures are necessary in order to protect these assets from both internal and external security risks.

The Swedish Armed Forces' KSF v3.1 [1] (Krav på IT-säkerhetsförmågor hos IT-system, English: Requirements for IT security capabilities of IT systems, see Appendices A, B, and C) contains the set of requirements, produced by the Military Intelligence and Security Services (MUST) [2] which have to be met by all IT systems in order to provide satisfactory protection of information in IT systems. KSF v3.1 presents a set of *functional* and *assurance* requirements which have to be met in order to decrease or eliminate the expected security risks [1] (see Appendix A, Sec. 1.7.1-1.7.2).

Many IT companies offer security management solutions and selecting the best one is a challenging process. The assurance requirements that are stated in the KSF v3.1 were compared with the security management solutions offered in the market, and the solution that satisfied the most of these requirements was selected for further evaluation.

Each IT system is a set of one or more IT components, and some of these components influence the overall security of the system. Thus, it is important to have confidence in the security of these IT components in order to have confidence in the entire IT system. Component assurance level describes the level of the assurance required by the each security-related IT component [1] (see Appendix A, Sec. 1.7.1). In addition, KSF v3.1 states four different levels of assurance used for classifying IT components based on the required level of assurance [1] (see Appendix A, Sec. 4.3). A *component assurance process* must be used in order to approve an IT component to a certain assurance level. It is important to note that functional safety requirements [1] (see Appendix A, Sec. 1.7.2) were **not** investigated due to the scope of the thesis.

The final step of this thesis project was to construct and propose a component assurance process that may be used by the Swedish Armed Forces when approving a specific security-related IT component to a specific assurance level.

1.1 Background

This thesis concerns the component assurance process for the Swedish Armed Forces. However, several other tasks had to be done in order to gain a full understanding of the structure of the component assurance process. Figure 1-1 illustrates the tasks involved in the construction of the component assurance process. The first task, security management market research, was performed by analyzing the Gartner Magic Quadrants [3] market research reports. These reports are provided by Gartner, Inc. [4], a leading company in providing technology-related insights. Selection of the leaders in providing security management solutions was the second task. The next task was a comparison between the functional requirements stated in KSF v3.1 and the leading security management solutions. This outcome of this task was the selection of the most suitable solution. Finally, a component assurance process was constructed.

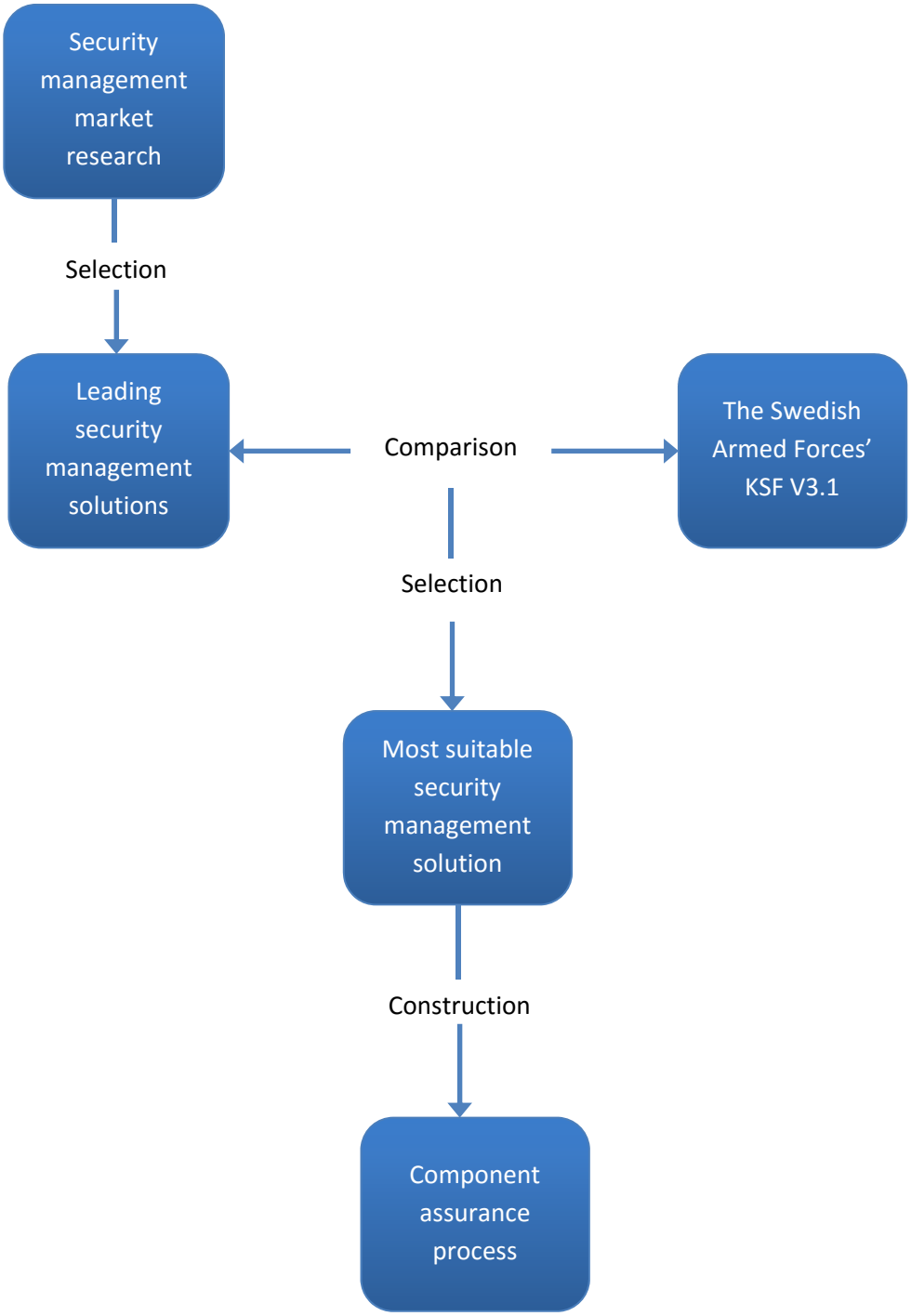

Figure 1-1: **Sequence of tasks required to carry out this thesis project**

1.2 Problem definition

Organizations and individuals are constantly exposed to various security threats. Protecting organizations from these treats is becoming increasingly demanding because of the growing interest of attackers in the organization's assets. The armed forces store a lot of confidential information that has to be protected from both insider and outsider attacks; hence the armed forces need to implement an appropriate security management solution. There are various approaches to security management and many companies offer their solutions/products to companies that need a security management system. The Swedish Armed Forces have a set of requirements that have to be met by their IT systems in order to maintain the desired level of confidentiality [1] (see Appendix A). The problem addressed by this thesis project is to select the most suitable security management solution and modify it, such that it fully meets the stated requirements. These requirements are specified in KSF v3.1, which itself is based on both Swedish laws and the Common Criteria [5] used to construct security requirements concerning IT security and for unbiased assessment of IT security. A component assurance process is a set of procedures *outside* of KSF v3.1. *Usage of a component assurance process during the development and production of a solution/product is essential.*

1.3 Purpose

The purpose of the thesis project is to produce a component assurance process that is simple and easy to understand. The Swedish Armed Forces proposed this thesis problem and therefore, the results of this thesis project should be beneficial for them. They might use the outcome of this thesis, i.e. the component assurance process, when approving a certain solution or product as meeting a stated component assurance level. This component assurance process will be essential for any company developing components to be sold to the Swedish Armed Forces or other organizations with high security requirements. Additionally, the results of this thesis project may be relevant to many organizations to help them define their own component assurance process for their own IT systems and for the IT systems of those who provide them with essential services involving confidential information.

1.4 Goals

The goal of this project is the definition of the component assurance process such that all the solutions/products developed and implemented following this process can be approved as meeting a stated component assurance level. This has been divided into the following sub-goals:

1. Perform a detailed security management market research and select the two leading solutions.
2. Compare the two leading solutions with the KSF v3.1 and its assurance requirements.
3. Select the solution that meets the most of the requirements for the further study and propose new functionalities for this solution. Possible changes to the existing functionalities should also be suggested such that the resulting solution would meet the requirements of KSF v3.1.
4. Construct a component assurance process.

1.5 Research Methodology

The thesis will use the empirical model in order to gain knowledge by means of direct and indirect observation or experience. A part of the thesis, concerning the market research, will involve Gartner Inc.'s methodology [4] used when they produce their Gartner Magic Quadrants [3]. The type of research and time duration of the overall thesis project was considered when choosing the appropriate methodology. More detailed information regarding the actual methodology and Gartner's methodology can be found in Chapter 3.

1.6 Delimitations

This thesis will not go into the details of the many security management solutions on the market today. Each solution takes a considerable amount of time to analyze, hence only two solutions were selected for the detailed analysis.

The selected security management solutions will **not** be tested running on actual hardware. The analysis and comparison will be performed based on the *specifications* provided by the companies and the KSF v3.1. Finally, functional safety requirements are **not** investigated in this thesis project.

1.7 Structure of the thesis

Chapter 2 presents the relevant background information about information security and security management. The purpose of this chapter is to give the reader the necessary background of these fields and introduce the reader to all the concepts necessary to understand the following chapters. Chapter 3 introduces the methodology and focuses on the security management market research that revealed several different security management approaches. Chapter 4 presents the two selected security management solutions and gives a detailed description of each of them. Chapter 5 compares these solutions with the requirements stated in KSF v3.1. The purpose of this chapter is to select the solution that most satisfies the requirements. It analyzes the selected solution in order to improve it so that it fully satisfies the KSF v3.1 requirements. Chapter 6 presents the component assurance process. Chapter 7 presents conclusions, a discussion of the limitations encountered during the thesis project, predictions for the future work, and some reflections.

2 Background

This chapter will provide the reader with all the relevant background information needed to understand the following chapters. The reader is introduced to both security management concepts and principles, and three security management approaches.

2.1 Security Management Concepts and Principles

The focus of the thesis is to explore various security management approaches in order to select the best solution for the Swedish Armed Forces. However, it is important to be familiar with the main information security and security management concepts before considering the different security management approaches.

According to SANS Institute™*: Information Security Resources [6], information security concerns the procedures and methods that are invented and executed for purpose of protecting confidential data or information from unapproved access, misuse of data or information, unauthorized disclosure, or alteration. Information security management represents an organized and regulated set of activities that implement and manage information security in an organization [7]. The degree of confidence that the information system's security components, applications, methods, and design implement the stated security policy is known as assurance [8].

2.1.1 Information Security Concepts

The three fundamental information security concepts are confidentiality, integrity, and availability (CIA) [9]. The CIA triad is a term very frequently used to denote these three concepts [10]. This triad is shown in Figure 2-1.

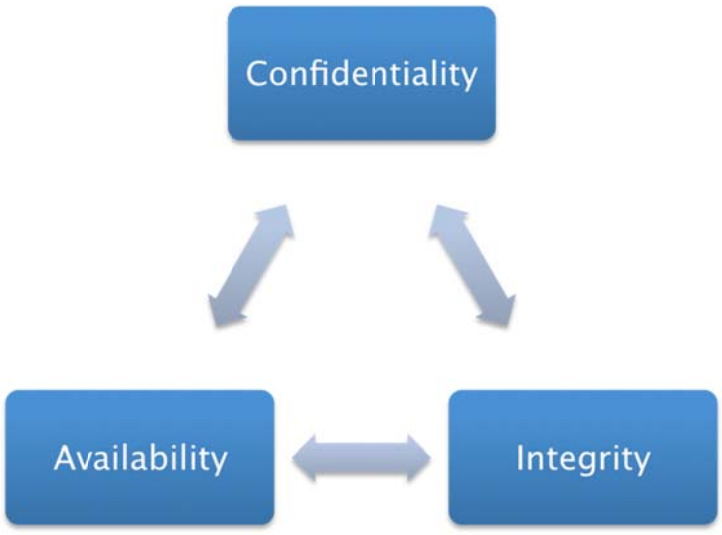

Figure 2-1: CIA Triad

* Escal Institute Of Advanced Technologies, Inc. doing business as SANS Institute.

As stated in SANS Institute: Information Security Resources [6], confidentiality is ensured by not revealing information to the unauthorized users. According to William Stallings this information security concept is the most susceptible to attacks, with a loss of confidentiality leading to the unauthorized disclosure of information [10]. According to Darril Gibson [11], access control mechanisms and encryption are deployed to guard against the loss of confidentiality. Access control is enforced by prompting the user to enter their credentials, and then these credentials are used to decide whether this person is authorized to use the resource(s). Encryption refers to the transformation of plain text data into ciphertext [11]. The reverse process of transforming ciphertext into the plain text data is referred to as decryption.

Integrity, the second component of the CIA triad, deals with assuring that the received data is the same as the original data, i.e., no data modification, insertion, removal, or replay has occurred [10]. A loss of integrity leads to unauthorized modification or destruction of data. According to Darril Gibson [11], hash functions are deployed to guard against the loss of integrity. A hash value, the result of the hash function, is a fixed length value that is used as a digital fingerprint of the plaintext. The receiver can apply this hash function on the received plaintext and then compare the hashes to check whether any data modification has occurred. The effectiveness of hash algorithms is based on the low probability of finding two plaintext messages associated with identical hash value [12]. According to William Stallings, a hash function should have the following properties: the function can be applied to any data block regardless of its size, the output of the function (hash value) must be of a fixed length, a hash value should be easily computed regardless of the complexity of the input, it must be computationally impossible to produce an input value based on the hash value, finding an alternative input that generates the same hash value as the original input must be infeasible to do (weak collision resistant property), and it should be computationally infeasible to discover any pair of inputs that yield the same hash value (strong collision resistance).

Availability ensures that data is available to an authorized user at any time. Therefore, a loss of availability leads to an interruption in access to data or an information system [10]. According to Darril Gibson [11], organizations deploy various methods to guard against the loss of availability and some of these methods are deploying fault tolerant systems, adding redundancy, and making backups. Fault tolerance means that a system can operate even if it develops a fault. Redundant drives and servers are used to realize fault tolerant systems. Backing up data is important should the original date become corrupted.

Various types of security attacks exist and providing protection against them is a challenging task. The purpose of each security attack is to cause a loss of one or more CIA triad components. According to ISO/IEC 2009 [13], an attack is an effort to demolish, uncover, modify, inactivate, steal, or acquire unlawful access to assets or perform unlawful usage of assets. Moreover, an asset is described as anything that is significant to a particular organization or company [13]. RFC 2828 [14] classifies each attack as either an active or passive attack. The goal of an active attack is to make a modification of assets or to disturb their functioning. Conversely, passive attacks do not modify the assets, but instead take advantage of them by using the available information [14]. As stated in William Stallings' book *Cryptography and network security* [15], active attacks are challenging to counteract due to the extensive range of susceptibilities. However, active attacks are easier to detect; therefore, the focus is on detecting them and recuperating from their effects. In contrast, it is very difficult to detect passive attacks because no modification of the assets is performed. Fortunately, preventing passive attacks is easier to achieve than preventing active attacks, and the main prevention against passive attacks is to use encryption [15]. In summary, active attacks focus on compromising integrity and/or availability, while passive attacks compromise confidentiality.

Attackers are classified as either insiders or outsiders. According to R. Lehtinen, et al. [16], multiple methods of system penetration are used by outsiders. Some of these methods are unauthorized access to an organization's facilities, unauthorized access by using networking devices,

offering a bribe to one or more of the organization's employees, and threating employees. According to William Stallings, outsider attacks are easier to detect than insider attacks [15]. Unfortunately, it is estimated that roughly 80% of attacks are performed by insiders. These attackers are employees who use their access rights to cause harm to the organization or bring gain to themselves by performing unauthorized actions. Moreover, insiders can also unintentionally cause harm to the organization by being reckless [16]. As stated by William Stallings in [15], it is much more demanding to discover and counteract insider attackers because they already have access and are familiar with the organization's structure.

2.1.2 Information Security Management Concepts

Information security management represents a systematized procedure that focuses on the execution and continuous management of information security in organizations. Information is extremely important for each organization and thus, information security management is needed in every organization. The goal of information security management is the protection of information and more importantly, the protection of the organization's information flow [17].

According to Bel G. Raggad, information security management has the following three capabilities [18]:

1. Precisely detects the computing environment of an organization.
2. Detects security threats and risks, and weakens them with the use of a risk security program.
3. Deploys an automatic review of the risk security program to continuously advance the organization's risk position.

Raggad goes on to say that evaluation of the organization's assets and revision of the risks with regard to present threats, susceptibilities, and consequences caused by the threats to the assets is necessary in order to successfully accomplish information security management Also, certain stages that have to be realized and finally, improvements have to be suggested.

Information security management is implemented by performing the following security activities:

1. Security planning whose goal is to outline the security requirements of a company by proposing administrative, functional, and technical security controls necessary for the organization in the following three years [18].
2. Development and revision of a security policy, which as the name suggests focuses on the assessment of security policies [18]. C. Paquet [19] defines a security policy as a collection of an organization's objectives, behavior guidelines for both the users and supervisors, and system and management requirements. The objective of the security policy is to guarantee the overall security of an organization. In addition, the process of creating a security policy is continuous due to the changing nature of the requirements [19].
3. Security risk analysis is required in order to devise security controls [13]. The purpose of this activity is to detect potential risks by using available information, and then to determine the probability of the occurrence of these risks. Furthermore, the consequences of the risks are also analyzed [20].
4. Security assessment is needed in order to perform a security risk analysis [13]. The aim of this activity is to ensure that the required security controls are incorporated into the project's design and implementation. The outcome of this activity is a document that

describes security holes between a project's design and the organization's security policies [21].

5. Security auditing is employed in various scenarios, such as forensic analysis, administrative compliance, supervising user activity, and troubleshooting. A rigorous group of security-related rules is implemented in many organizations, often as posed by industry regulations. The goal of security auditing is to assist in the implementation of the organization's security policies and to verify their implementation [22].

6. Security certification and accreditation describes the process of certifying that a certain information system satisfies the stated security requirements, and later on accrediting that system. In addition, a guarantee that the system will uphold accreditation during the system's entire life cycle has to be provided [23].

7. Information Security Management System (ISMS) development is performed based on ISO 27001 [24]. As stated by Raggad in [18], an ISMS represents a risk related security program developed for an organization. The security controls from the ISO 27001 standard are used to establish the security controls in the ISMS. Before this, the system's scope and security policy are explicitly stated. Moreover, the risks are determined, analyzed, and reduced prior to the construction of a risk related security program and a statement of applicability [19]. Section 2.2 discusses risk management.

8. Intrusion detection deals with observing events in a system and investigating whether a violation of security policies has occurred [25]. It is important to detect an intrusion rapidly in order to remove the intruder from the system before damage has occurred or to prevent major damage. Intrusion detection quantifies the difference between an intruder's and a legitimate user's behavior patterns. However, this difference is often unclear and some intersection is always present [10].

2.1.3 Information Security Policy Framework

According to Harris in [26], in order to have effective security mechanisms in an organization, all levels within the organization have to be involved, and the security functions must be functional and useful in every level. The responsibility of the senior management is to state the range of security and to identify those assets that require protection from various security threats. Thus, management has to be familiar with the rules, constitution, and legal responsibilities concerning the security that their organization needs to provide, and then they must act in such a way as to guarantee that all of the requirements are met. In addition, the security management team needs to define a set of rules concerning all of the employees and their behavior.

Some of the elements of an effective security program are security guidelines, procedures, policies, and standards that form security documentation. This security documentation has to be constructed with regard to the type, culture, and objectives of a specific organization [26].

A policy is a document that expresses a general statement of senior management. The aim of a security policy is to describe the position of security mechanisms inside a particular organization [27]. According to InfoSec Institute [28], employees have to read through these policies in order to gain an understanding of what is expected from them regarding usage of the organization's information systems. As stated by Harris in [26], many types of policies exist, but all of them aim to protect an organization's assets. He goes on to describe some of these different types of policies. Regulatory policies are used to confirm that the organization complies with the standards specified for a certain industry. Advisory policies describe employees' expected behaviors and activities within a specific organization. Informative policies provide notifications about

particular subjects to employees in order to educate them about the topics that are important to the organization.

A standard contains a collection of rules concerning the development and management of materials, products, services, technologies, and systems [20]. According to a posting by Paul Johnson on MindfulSecurity.com [29], standards assist in the implementation of security policies and they provide support by ensuring security stability within an organization. A number of universally recognized information security standards exist, and some of them focus on information security management. The ISO/IEC 27001 standard [30] provides a list of requirements for the formation, implementation, maintenance, and enhancement of ISMS. The Plan-Do-Check-Act (PDCA) model was introduced in the 2005 version of the standard (ISO/IEC 27001:2005) with the objective of structuring the processes and presenting the concepts of the Organization for Economic Co-operation and Development (OECD) Guidelines. The OECD Guidelines [31] describes a set of recommendations for multinational enterprises. They were constructed by governments in order to deliver principles and standards of good practice in agreement with the appropriate regulations. The Common Criteria (ISO/IEC 15408) [32] is another internationally recognized standard that guides the development of IT security related products and systems. Furthermore, it serves as a guide for obtaining security-related commercial products and systems. The objective of the Common Criteria is to perform an assessment of security-related products and systems, which later leads to providing assurance.

A guideline is a document that describes suggestions for best practices; hence it is useful in situations when a standard cannot be utilized. While standards represent compulsory instructions, guidelines are wide-ranging methods that can be applied in unexpected situations [27]. An example of a standard is that passwords must meet specified complexity and length requirements, while a guideline supporting this standard could state that passwords are no longer valid after a certain amount of time [29].

Procedures describe the implementation of policies, standards, and guidelines in an organization. Furthermore, these procedures provide a detail explanation of the tasks involved in achieving a particular goal [27]. An example of a procedure is an explanation of how to install a Microsoft Windows operating system by describing the tasks necessary to fulfill the relevant policies, standards, and guidelines [29].

Figure 2-2 illustrates an information security policy framework that consists of four levels representing the above-mentioned types of security documents. Although every level of the framework supports the levels above it, these levels should never be merged - as each level targets a different group of people [29]. According to a posting by Paul Johnson on MindfulSecurity.com, the following example describes the functions of the framework's levels and how they depend on each other [29]:

- A policy focuses on the protection of sensitive information by classifying the information that must be protected during a transfer of this information.
- A standard supports a policy by requesting that a particular encryption algorithm should be used and that a log of all transfers should be kept.
- A guideline supports both the standard and policy by describing the best practices for making a record of sensitive information transfers and providing models for the transfer log.
- A procedure describes detailed directions for the encryption of sensitive information such that the successful completion of the stated actions guarantees compliance with the above-mentioned documents. Procedures represent the lowest level since they are the most detailed and they must be comprehended by a large number of people.

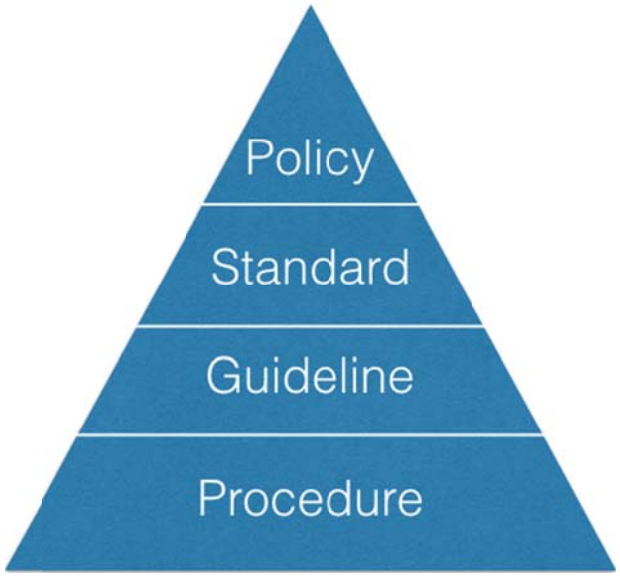

Figure 2-2: Information Security Policy Framework

2.1.4 Security Attacks

Section 2.1.1 described the difference between active and passive attacks, both in terms of their nature and the ease of discovering them. Moreover, attackers or intruders were described as either being internal to or external to the organization. This section will focus on several potential security attacks in order for the reader to gain insight into a number of scenarios that could cause harm to the organization.

Successful attackers will perform some investigation before actually attacking the system. "Footprinting" [33] represents the initial step taken by attackers in order to accumulate information about the targeted organization and its system. The objective of the attacker is to study the organization's security structure and position, gain insight into their Intranet and remote access possibilities, etc. The goal of these activities is to discover the organization's security flaws. Numerous tools and technologies can be used to perform footprinting; thus, it is necessary for the security personnel of the company to be acquainted with them so that they can recognize them and mitigate them.

A virus is a program designed to transmit malicious code. This code infects computers and further spreads the virus. Certain viruses are hidden and a user may not notice that his computer is infected, while others make alterations to data residing on the computer or negatively impact the system's performance [34]. There are many ways of spreading a computer virus, such as inserting a virus into an e-mail attachment or by downloading files or programs from the Internet that are infected by a virus. For this reason it is very important to **not** open attachments sent from unknown people and to be careful when downloading files or programs from the Internet. Many methods can be employed in order to circumvent viruses, such as updating the computer with the current software updates, installing antivirus programs, running the computer in the standard user mode, and being careful when downloading files, programs, and attachments [35].

A worm is a program designed to make a copy of itself, and then spread that copy across a computer network. Similar to a virus, a worm implements malicious code with the goal of utilizing the computer's assets and probably making the system shutdown. The key distinction between a worm and a virus is that a virus attacks one computer and then transfers itself to the next computer, while a worm remains on the computer until it runs out of space (or other resources). This feature

makes worms extremely harmful when they spread on the Internet [36]. There are many ways of infecting a system with a worm and most of them are the same methods as used for spreading viruses. The main indications of a presence of the worm in a system are poor system performance, system freezing or crashing, involuntary opening and running of programs, getting unexpected firewall notifications, disappearance and alteration of files, presence of odd files and icons, receiving unexpected system error messages, … [37].

IP spoofing [38] is an attack that focuses on obtaining unauthorized access. This type of attack makes use of the vulnerability in the Internet communication that occurs between the intermediate routers that are involved in delivering a packet from a source address to a destination address. The intermediate routers discover the best route by reading the destination address in the packet's header, but usually do **not** inspect the source address. Only the destination host inspects the source address when replying back to the source host. Thus, an intruder, who employs an IP spoofing attack, sends a message to the destination host with the source IP address field belonging to a trusted host. However, in order for the attack to be successful, the intruder first has to discover the source IP address of a trusted host, and then alter the packet header of a packet to include this address. The ultimate goal is to obtain access to the host by spoofing the host into thinking that the packet came from a trusted source.

A Denial-of-Service (DoS) attack focuses on preventing authorized users from using a particular service. Some of the ways of achieving this attack are flooding the network in order to block the authorized network traffic, interrupting the connection between hosts, blocking a specific person from using a certain service, etc. The goal of a DoS attack is to make the information assets of a particular target less useful or important. With respect to the CIA Triad, DoS attacks mainly affect availability [39]. The occurrence of DoS attacks has been noticed for decades. Moreover, an extension of this attack, known as Distributed Denial-of-Service (DDoS), has been present since 1999. The difference between these two attacks is that in a DDoS attack the packets that are trying to prevent the legitimate user from using a particular service arrive from various addresses as opposed to single source addresses as in a DoS attack. As a result, DoS protection that focuses on observing packets arriving from a single address or network will not function against a DDoS attack [40].

According to the S. McDonald of SANS Institute, SQL injection attacks exploit vulnerabilities in the system's code to pass commands to the system's database in order to enable the attacker to access the system [41]. Attackers use SQL injection to perform various attacks, such as logging in to an application with invalid credentials, acquiring data from the database, modifying data, adding malicious data, deleting log or audit data, … [42].

Password attacks focus on acquiring users' passwords. As stated by Roger Grimes in [43], there are many types of password attacks and becoming familiar with them might prevent their success. Some of these attacks are [43]:

- Password guessing is the mostly used type of a password attack. A manual or automated method of password guessing can be utilized. The passwords can be guessed either locally or remotely. This attack has a high probability of occurrence because many networks do not force users to use lengthy and complicated passwords. Moreover, an attacker simply has to guess one weak password in order to access the network. Automated methods of password guessing can utilize several approaches: A brute-force attack is the most effective and slow approach, as it focuses on trying all potential passwords by considering the character set and restrictions on password length. Another approach is a dictionary attack that assumes that most passwords include complete words, dates, or digits from dictionaries. Thus, dictionary attacks need a suitable dictionary as an input.

- Password resetting is used because a lot of times it is simpler to reset the password instead of guessing it. Numerous password-cracking programs perform password resetting.
- Password cracking is preferred over password resetting because attackers typically want to learn useful passwords, without tipping the real user off that their account has been compromised. This method consists of obtaining a password hash, and then transforming it to the plaintext original. However, an attacker requires tools for hash guessing in order to crack a password. Also, rainbow tables are required for plaintext passwords and passwords sniffers for extracting the authentication data. It is important to emphasize that these types of attacks can succeed when the password hashes are not good hash functions.
- Password capturing is a method of obtaining passwords by using keyboard sniffing, a Trojan horse, or some other keyboard-logging device.

Numerous types of attacks exist, and protecting an organization from them has become a very challenging task. It is very easy to become a hacker nowadays due to the many tools that can be downloaded from the Internet. In contrast, in the past only programmers with excellent skills could become hackers. The availability of attack tools and mostly open networks have attracted many bad people to attack organizations and individuals. However, this phenomenon has also increased the demand for enhanced security and security policies. Protecting the network from outsider attacks can be relatively simple. The most efficient technique is to use private networks that have no connections to public networks, as these networks are thought to be safe from outsider attacks. However, it is estimated that majority of the network attacks are actually performed by insiders which makes providing protection much more complicated [44]. Moreover, there are many security professionals who regard isolated networks as actually being connected, but having a high delay.

2.2 Security Management Approaches

The first task of this thesis was to perform market research regarding security management. Cyber security companies are experiencing an extraordinary growth, and continue to develop new software products and services. Choosing the most suitable solution for a specific organization can be a challenging process due to the extensive number and variety of offers, and the fact that each organization often believes that it has different characteristics and needs than other organizations.

This thesis project investigated the three most popular security management approaches: Security Information and Event Management (SIEM); Governance, Risk Management, and Compliance (GRC); and Identity and Access Management (IAM). This section explains the principles and concepts behind these three approaches, while the description of those solutions available in the market will be given in Chapter 3.

2.2.1 Security Information and Event Management (SIEM)

Security Information and Event Management (SIEM) is a security management approach whose aim is to offer a complete perspective of an organization's security in terms of information technology. The core basis behind SIEM systems is managing an organization's security from a single location. The data concerning the security of an organization is usually spread across various locations, thus making it difficult to notice abnormal trends and patterns. For this reason SIEM products and services focus on gathering all of the data in one place, and then analyzing it.

As stated by Harold F. Tipton and Micki Krause in [45], SIEM products and services merge Security Information Management (SIM) and Security Event Management (SEM) operations inside

a single security management approach. According to Hervé Debar and Jouni Viinikka in [46], SIM solutions have four functions: event acquisition, contextual information management, alert correlation, and reporting. The purpose of event acquisition is collection and transfer of events to a central location responsible for additional processing. Contextual information management deals with guaranteeing the proper attachment of contextual data to hosts and users. In addition, this function is responsible for handling modifications in the contextual data in order to maintain up-to-date and accurate data. Alert correlation is in charge of prioritizing alerts that should be forwarded to security officers; hence this function is necessary for ensuring that the most crucial alerts are processed first. Lastly, the purpose of reporting is to provide several interfaces to those responsible for information retrieval. In contrast, SEM solutions are computerized tools responsible for storage centralization and analysis of logs and events produced by SIMs and SIEMs [47]. Thus, SIEM solutions help the security and system personnel when analyzing, regulating, and controlling the organization's information security structure, policies, and procedures. As stated in John R. Vacca's book *Computer and Information Security Handbook* [48], SEM solutions concentrate on real-time examination, event correlation, and provide notification and console views. Conversely, SIM solutions collect data in a long-term repository, and afterwards use the collected data for analysis and log reporting. Thus, according to Adam Gordon and Steven Hernandez in [49], the purpose of combining SEM and SIM operations is to have a complete view of the organization by using log collection, normalization, correlation, aggregation, and reporting. Moreover, this combination permits confirmation of fulfillment of an organization's compliance requirements by the compliance managers.

According to Harold F. Tipton and Micki Krause [45], most SIEM solutions offer the following functionalities:

- *Log aggregation* is deployed for collecting log output from the network and storing it into a single console.
- *Log storage* stores gathered log data in a log server.
- *Real-time threat analysis* analyzes log data and notifies security personnel about existing threats. Threats are identified based on a combination of log data.
- *Historical data retrieval* enables security personnel to retrieve historical log data in order to ensure that devices are functioning properly, organization's information security policy is followed by users, etc.
- *Network's topology demonstration* is useful for visualizing the location of threats, and identifying hosts and devices that are in the region of the existing threats.
- *Critical status indicators demonstration* provides a visualization of attack rates and types by using pie charts, line graphs, and dashboards.
- *Cases creation* allows users to gather information regarding incidents, and share that information with incident response effort members.
- *Workflow tracking* is used to outline the steps required for incidence response, and to verify that those steps are completed.
- *Compliance verification* provides report used for verifying that an organization has complied with certain regulations.

As stated by Mark Nicolett and Kelly M. Kavanagh in Gartner, Inc.'s 'Critical Capabilities for Security Information and Event Management' [50], having a SIEM system is a critical component in developing a security plan for an organization. A SIEM system utilizes a central location where security monitoring is performed and attacks are detected in their initial stages, and thus, the

damage is potentially reduced. This is achieved by supervising user activity and data access, reporting detected threats, and employing methods for satisfying audit requirements. Thus, SIEM solutions offer the following capabilities [50]:

- Internal and external threat discovery,
- Monitoring privileged users' activities,
- Monitoring server and database access,
- Monitoring user activity and then correlating and analyzing this activity from various systems and applications,
- Compliance reporting, and
- Performing incident response analysis.

2.2.1.1 SIEM Concepts

This section discusses the components of a SIEM solution and the concepts behind them.

a) Log Management

The foundation of every SIEM system is a log management system that collects events and aids in extracting useful information from those events. According to David R. Miller, et al. [51], a few concerns regarding log management and its usage exist. The first concern is the time period of log retention. Certain industry regulations and laws place constraints on specific types of data and the amount of time that data can be kept; this is known as *data retention*. Additionally, it may be required to discard specific data after a certain amount of time, and this constraint is known as *data destruction*. Another important question is how much log data must be retained, especially in large networks where the amount of data is vast. The volume of log and event data even in smaller networks will quickly exceed the available storage, if no limitations are imposed. Therefore, it is important to determine what sort of data needs to be retained, while considering the amount of storage available.

According to RFC 5424 [52], a *syslog protocol* is utilized to transport event notification messages. The layered architecture of this protocol permits the usage of any transport protocol for transmitting event notification messages. As stated in *Security Information and Event Management (SIEM) Implementation* [51], the majority of networking devices can produce syslog messages that are transferred to a central management console for processing and storage. These devices are usually configured to either a low or high reporting level, which means that the number of messages can be restricted. However, it is the task of a security administrator to determine which syslog messages are of interest for a particular organization, and to configure the devices accordingly.

Network devices also collect flow data, which provides information about certain data streams between endpoints. As an illustration, a client on a specific network demanding a web page from a server on the Internet usually generates a considerable number of syslog messages, but generates only one flow record. This flow record contains information about the two communicating devices, the volume of data transmitted, and what service was used. Thus, exploiting flow data can be very beneficial when collecting high-level views of traffic [51].

According to A. Williams and M. Nicolett in [53], Vulnerability Assessment (VA) is valuable for SIEM systems because it supports vulnerability management by providing discovery capabilities. There are many functions of VA products, such as endpoint scanning and determining vulnerable situations depending on known vulnerabilities that are stored in a database. Also, it is possible to resolve other endpoint characteristics, such as open ports, running services, protocols, applications,

operating system, etc. All of this information is very useful for the security personnel when measuring security postures. The elimination of the origin of the most exploits, reduction of the probable attack vectors, and restriction of the incident's impact can be considered only after the security personnel have identified the security limitations of a networking infrastructure.

b) Event Correlation

After collecting log and event information, it is necessary to use that information to draw some conclusions. Thus, some event and information correlation will be performed in order to relate the events and the other information.

Figure 2-3 illustrates the SIEM stack with the Event layer being the foundation for all the other layers. According to *Security Information and Event Management (SIEM) Implementation* [51], the purpose of the Event layer is log collection and the event messages gathering. The Normalization layer is where the conversion of messages to a standardized syntax occurs. Relating events to each other occurs at the Correlation layer, while the Reporting layer creates the output and takes actions depending on those events that have entered the SIEM system.

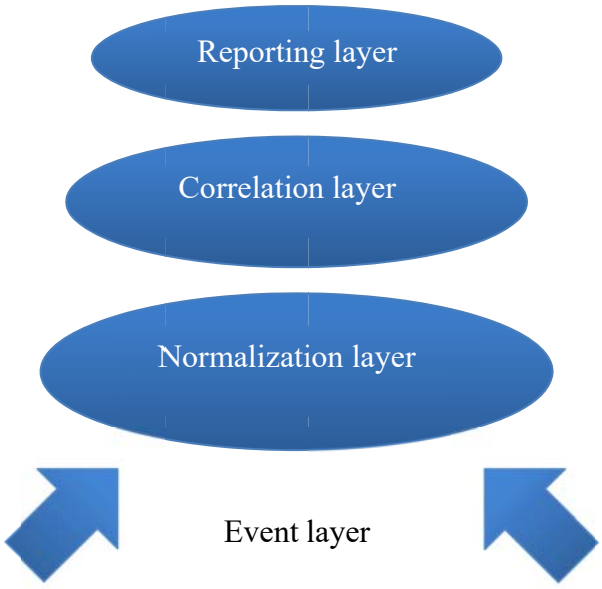

Figure 2-3: The SIEM Stack (Adapted from Figure 4-4 of [51])

c) Endpoint Security

Endpoint security is a capability of numerous SIEM systems, and it focuses on security supervision of various endpoints, mostly clients, from a central location or a management system. Additionally, it protects the network from these endpoints, such as portable computers, desktop computers, smartphones, etc. As stated in [51], the following fields of endpoint security are worth mentioning:

- Operating system (OS) and applications strengthening
- Antivirus and antispyware updating
- Firewall configuration
- Host Intrusion Detection Systems (HIDS) provide intrusion detection on a single host by establishing an agent program on that host that supervises and reports its activity and configuration. These systems have various capabilities, such as log analysis, event correlation, integrity inspection, policy implementation, rootkit discovery, … [54].

- Host Intrusion Protection Systems (HIPS) protect the hosts from the various attacks. As stated in SANS Institute InfoSec Reading Room [55], this protection is provided from the network layer to the application layer, and it is achieved by combining a personal firewall, intrusion detection system, anti-virus, etc.
- Configuration Management (CM) represents a comprehensive process of recognizing and describing configuration items, supervising the status of those items, handling requests for change, and validating the extensiveness and accuracy of the items [56]. According to IBM Knowledge Center [57], a configuration item represents any item, such as service component or infrastructure element, that requires managing for the purpose of successful service(s) delivery.
- Removable media management deals with controlling removable media, such as thumb drives, DVDs, and CDs, at the endpoints in the network. This managing is reflected through security measures, for instance, firm policies, security training, and technical regulations [51].
- Network Access Control (NAC) deals with managing access to networking assets. NAC performs authentication when users try to log into the network, and determines what assets and actions are accessible to each user [10].
- Network Intrusion Detection Systems (NIDS) scans for suspicious activities, such as attacks or illegal activities, by observing the traffic on the network segments [58]. According to Thomas and Stoddard in [59], HIDS and NIDS have different functionalities, and thus both are needed to increase the security of a network. In spite of their unquestionable importance, both HIDS and NIDS have some drawbacks that need to be discussed. The purpose of NIDS is to observe and analyze the traffic on the network. However, network sniffers are not able to analyze all the network traffic due to the switches that are installed in the network. Thus, a network sniffer can only analyze the network traffic traversing the segment to which it is attached. Furthermore, NIDS configuration can sometimes cause a large number of false positive alerts. One of the drawbacks of HIDS is the implementation complexity in large environments caused by several thousand endpoints each generating entries for log files.
- Network Intrusion Protection Systems (NIPS) protect computer networks by blocking the traffic coming from suspicious sources. According to J. Kissell in [60], even though both NIDS and NIPS share the same infrastructure, NIPS has an additional component responsible for preventing access to attackers. To be more precise, NIPS are usually configured to add a new firewall rule or take some other security-related action whenever a malicious traffic is identified.

2.2.1.2 The Structure of a SIEM

A SIEM system consists of a number of operational elements, with each element being in charge of a particular task. In order for the entire system to function accurately, all of the elements have to be correct, and work together. Many versions of a SIEM system exist, with each system having supplementary elements, but this section will describe a basic SIEM system.

As illustrated in Figure 2-4, a basic SIEM solution consists of six independent elements, and these elements are: the source device, log collection, log parsing or normalization, rule engine or correlation engine, log storage, and event monitoring. As stated in [51], every element can function independently, but a SIEM system will not function accurately without all the elements working with each other.

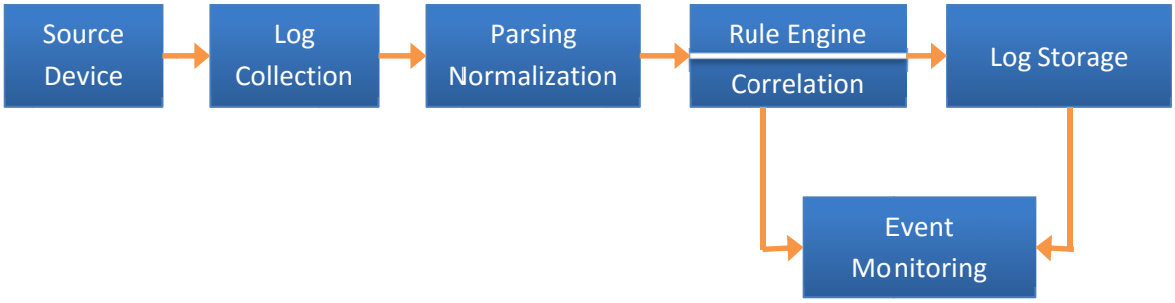

Figure 2-4: The SIEM Structure (Adapted from [51])

The source device is the first element of the SIEM structure, and it serves as an input to the SIEM system. According to David R. Miller, et al. in [51], any kind of a device or application can be a source device, as long as logs can be retrieved from it, and later stored and processed by the SIEM system. Thus, a source device is actually not a segment of the SIEM system that is purchased as part of the SIEM system, but rather it is essential for the purposes of the organization. A SIEM system cannot function without the logs and other information generated by source devices [51]. Thus, it is very important to analyze each organization in order to decide which devices are critical for the retrieval of their logs.

After selecting the source devices, it is essential to retrieve the logs from those devices and transfer them to the SIEM system. This operation is called *log collection*, and two essential techniques for log collection are the push and pull methods. The push method is utilized when a source device sends its logs to the system; while in the pull method, the system retrieves the logs from the source device(s). David R. Miller, et al. say that the advantage of using a push method is simplified setup and configuration of the SIEM system. In the most cases, only a receiver needs to be installed and the source devices directed to send their log data to this receiver. An example of a push method is the syslog protocol, where a source device needs to be configured with the IP address or DNS name of a syslog server on its network. This source device will then send log entries to the syslog receiver, which is actually part of the SIEM system. However, a drawback of using a push method is that it can introduce some security issues. An example of such a security issue occurs when using the syslog protocol over the UDP protocol. Because UDP is a connectionless protocol, it is not guaranteed that packets containing the logs will reach the destination server. In contrast, a disadvantage of using a pull method is that logs might not arrive at the SIEM system in real-time [51].

The next element of the SIEM structure is *normalization*, which deals with the conversion of logs to a single standardized format. The outputs of the previous element, log collection, were logs that are in their original format, but these logs are not useful to a SIEM system and thus, have to be normalized. Figure 2-5 shows an entry from a Windows event log and Figure 2-6 shows a Cisco ASA syslog message, both illustrating an event of a user logging to a system. However, it is obvious from these figures that different vendors use different formats for representing their logs. Thus, in order to understand the events, it is necessary to convert them to a common format. Figure 2-7 illustrates both of these logs (Figure 2-5 and Figure 2-6) after the normalization procedure. Normalization is not only useful for enhancing the readability of the events, but also for enabling a standardized rule format [51].

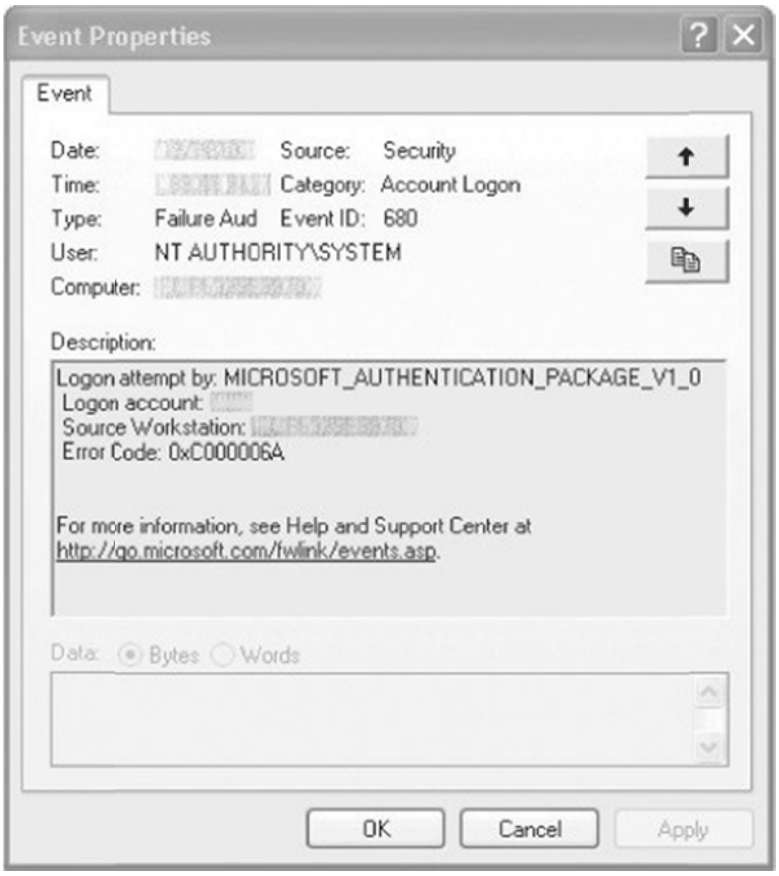

Figure 2-5: **Windows Event Log (Adapted from Figure 5-1 of [51])**

Priority	Hostname	Message
Local4.Info	192.168.1.1	:%ASA-sys-6-605005: Login permitted from 192.168.1.18/42925 to INSIDE:192.168.1.1/

Figure 2-6: **Cisco ASA Syslog Message (Adapted from Figure 5-2 of [51])**

Time	Date	Source Device IP Address	Event Message	Event
22:54:53	CST 17-Jan-10	192.168.1.1	User login	ASAsys-6-605005
22:54:53	CST 17-Jan-10	192.168.1.18	User login	Security: 680

Figure 2-7: **Normalized Events (Adapted from [51])**

A rule engine is used for activating alerts based on certain conditions occurring in the normalized logs. Boolean logic is usually used for writing the rules and deciding whether particular conditions are met [51]. Figure 2-8 demonstrates the administration login rules, where an alert is activated when a local administrator logs into a server. A subset of a rule engine is responsible for matching several events into a correlated event, thus this subsystem is known as the correlation engine. Correlation is performed to make incident response procedures simpler. Thus, only one event is triggered when several related events arrive from several source devices.

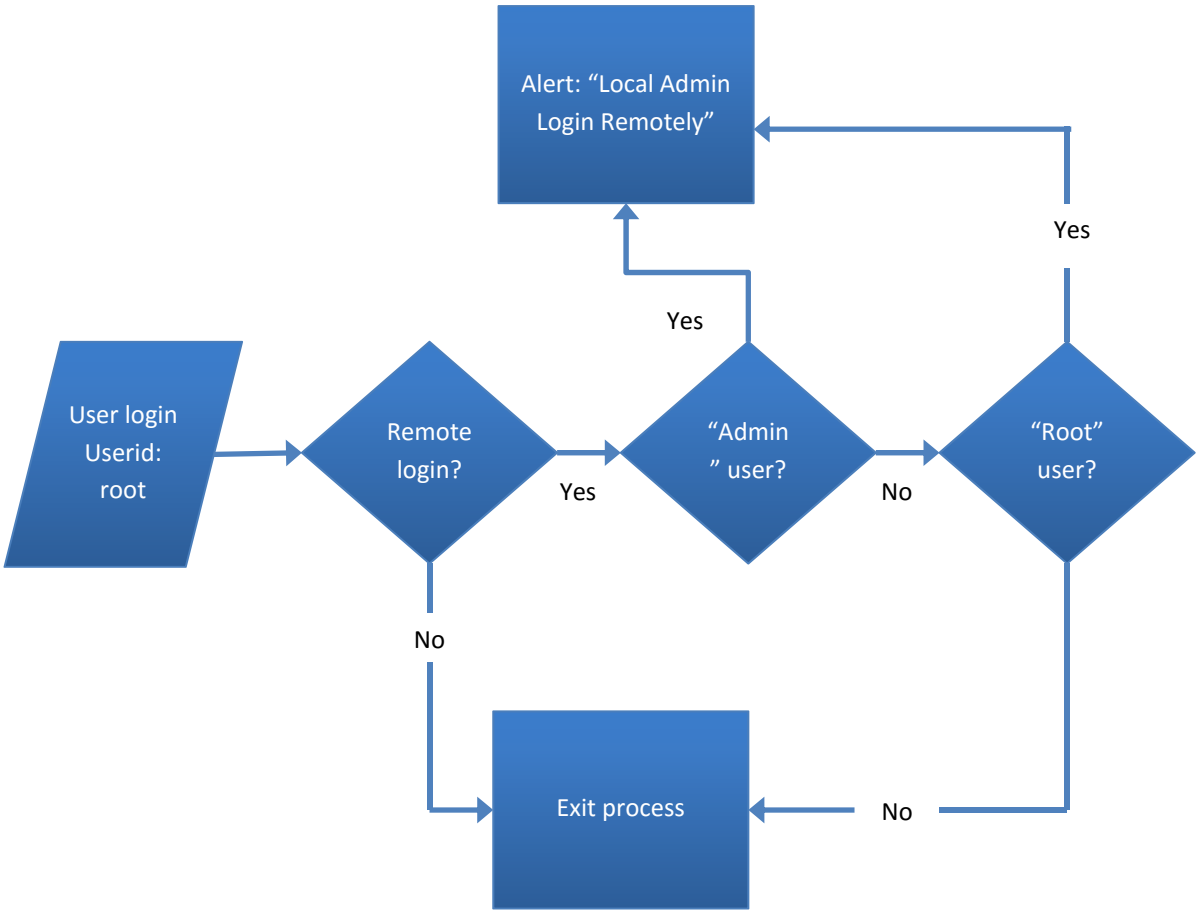

Figure 2-8: Admin login rules (Adapted from Figure 5-3 of [51])

Log storage is used to accumulate numerous logs that arrive to the SIEM system. These logs have to be stored for the sake of retention and historical queries. Three methods of log storage are typically utilized, and those are: database storage, flat text file storage, and binary file storage. Database storage is the most common method of storing logs due to the simple methods for interaction and data retrieval. Typical database platforms, such as Oracle, MySQL, Microsoft SQL, etc., are used for storing the data. Flat text file storage utilizes text files to store the data in a human-readable format. However, this method is not utilized frequently due to its poor performance and poor scaling. Binary file format stores binary data, but is only utilized by certain SIEM systems.

Event monitoring is the last element of a basic SIEM solution. This stage is used for exploitation of the logs that were stored in a SIEM system in the previous stage. The purpose of event monitoring is to use the stored data and benefit from it. An interface for event monitoring is provided, which provides an overview of the entire environment.

2.2.2 GRC (Governance, Risk Management, and Compliance)

Governance, Risk Management, and Compliance (GRC) is a security management approach covering three concepts: governance, risk management, and compliance. Many definitions of this security management approach exist, and some of them have different perspective of what GRC stands for. According to KMPG [61], one of the four largest international accounting companies, GRC represents a continuous process responsible for protection against security-related risks, supervision and estimation of internal controls efficiency, and improvability of operations by using the learned insights. Moreover, it is stated that GRC is not simply a software solution, but rather a strategic method that produces business value through cost reductions, identification of operational inefficiencies, controls rationalization, risk identification, and risk management. As R. Banham points out in [62], GRC represents a technology platform responsible for illumination of governance and compliance risks. According to OCEG [63], a global nonprofit policy institute that invented the acronym GRC, the three terms constituting this acronym represent concepts that have been used for a long time. However, GRC represents much more than a union of these concepts into an acronym. According to P. Proctor [64], a Chief of Research for Risk and Security in Gartner, Inc., the acronym GRC represents a very useless term because it is used by vendors to promote anything that they sell, and clients use it without knowing what it actually stands for. He also indicates that GRC should not be interpreted as a project or a technology, but rather it represents a collective intent of enhancing governance by means of a more efficient compliance, and a greater knowledge concerning risk impact on organization's performance. Even though a formal definition of GRC does not exist, it can be concluded that GRC represents a security management approach whose aim is to improve the organizations' performance, and that it represents more than just a software solution.

As stated in research conducted by Ponemon Institute, GRC activities usually belong to one of the following domains [65]:

IT GRC This domain deals with the management of IT-related controls, which incorporate security-related controls (firewall, security information management system, etc.), system controls automation, susceptibility supervising tools, identity management system, access management system, disaster planning and management, and disaster recovery systems.

Operations GRC Management of an organization's fundamental operations is handled in this domain. For instance, it is important for an organization to guarantee that support for managing processes from various systems, such as Human Resources and manufacturing systems, exists.

Finance GRC This domain focuses on the financial controls management. Some of the activities of this domain are management of conflicting permissions by assessing the separation of duties, and analysis of process-related business rules.

Legal GRC Management of regulatory compliance controls and contractual requirements is handled in this domain. Organizations have to guarantee accurate corporate governance reporting management, anti-fraud, anti-corruption, privacy protection, etc.

As previously mentioned, a part of the thesis uses Gartner Magic Quadrants produced by Gartner, Inc. for performing a market research. According to John A. Wheeler in [66], Gartner, Inc.'s OneGRC research program responsible for evaluating GRC market and its segments has defined the following market segments within GRC:

IT Risk Management	This market segment deals with the IT risks that fall under the responsibility of the IT department, risks caused by insufficient or unsuccessful internal IT processes, or risks resulting from external events. Thus, the activities involved in IT Risk Management are IT risks evaluation, policy management, security operations evaluation and reporting, incident management, and compliance mapping and reporting.
Operational Risk Management	According to Bank for International Settlements, operational risk is "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events" [67]. Hence, the activities involved in Operational Risk Management are aggregation and normalization of data coming from various sources, such as operational systems, financial systems, regulatory events, loss event databases, etc.
IT Vendor Risk Management	This market segment tackles the risks associated with the regulatory compliance and information security. As a matter of fact, these risks emerge through the use of services provided by third-party IT service providers and IT vendors.
Business Continuity Management Planning	The goal of this segment is to identify the risks that might cause business disturbances, implement the disaster recovery system, react to disturbing events, and recuperate organization's vital business processes. Thus, this market segments focuses on the activities such as risk assessment, business impact analysis, recovery plan development, etc.
Audit Management	Audit Management market segment automates internal audit processes, such as audit planning, work paper management, time management, scheduling, cost management, reporting, etc.
Corporate Compliance and Oversight	The goal of Corporate Compliance and Oversight market segment is to help compliance leaders by supporting their actions. Hence, the activities involved in this segment are compliance risk assessment, regulatory change management, investigative case management, control validation, etc.
Enterprise Legal Management	The Enterprise Legal Management segment aims to help legal and compliance departments, directors, secretaries, and senior management by providing improved documentation, cost management, information availability, e-billing, legal document management, etc.

Chapter 3 will analyze the Gartner, Inc.'s Magic Quadrants reports for the GRC market segments mentioned above. In order to gain a better understanding of GRC, the following sections will describe governance, risk management, and compliance.

2.2.2.1 Governance

As stated in Mark Bevir's book *Governance: A Very Short Introduction* [68], the term "governance" has been present everywhere since the 1980s. In fact, various source report about global governance, corporate governance, collaborative governance, environmental governance, etc. Hence, it is important to define the term "governance", and more importantly, what the term "IT governance" stands for. Bevir goes on to say that many definitions of governance exist; it is believed by some people that governance is simply an indefinite substitute for the term "government", others think that this term has been so over-used that it has lost its meaning, and finally the majority agree that governance is a logical idea that has proven to be very useful. According to United Nations Educational, Scientific, and Cultural Organization (UNESCO), governance represents "structures and processes that are designed to ensure accountability, transparency, responsiveness, rule of law, stability, equity and inclusiveness, empowerment, and broad-based participation" [69]. Hence, the term governance applies to all procedures of governing, no matter who is the source of it.

According to Gartner IT Glossary [70], the term "IT governance" represents a set of processes responsible for guaranteeing an effective and efficient utilization of IT with the purpose of helping organizations to accomplish their objectives. Furthermore, it is also noted that IT governance can be divided into two subgroups that are responsible for different processes. The process responsible for guaranteeing the efficient assessment, selection, ranking, and financing of competing IT investments is known as IT demand governance. In addition, IT demand governance helps organizations to manage their implementation, and to obtain their business profits. In contrast, IT supply-side governance is a process that deals with guaranteeing that the IT organization functions effectively, efficiently, and compliably.

As A. Tarantino points out in [71], companies' business existence and prosperity in most cases depends heavily on the use of IT, and that companies that do not invest in their IT will not experience any growth. Thus, IT governance is driven by the following factors [71]:

- Competitive advantage in an information economy that is dynamically changing is constantly being pursued. This competitive advantage is gained by using IT, and employees' knowledge, skills, and experience.
- Governance requirements stated by OECD are evolving at a high rate.
- Information and privacy statutory laws are expanding.
- Organizations' assets and IT are being exposed to an increasing number of security threats.
- Technology projects and strategic legislative objectives have to be aligned in order to provide their intended value.

The official standard for IT governance is *ISO/IEC 38500:2015 Information technology – Governance of IT for the organization* [72]. The focus of this standard is the organization's present and upcoming utilization of IT. This utilization comprises management procedures and assessments regarding the present and upcoming IT usage. Furthermore, the standard states that IT governance represents a subcategory of organizational governance, or corporate governance with regard to corporations. Hence, the objectives of ISO/IEC 38500:2015 are the following:

- Presenting the values and applications of the standard to directors, and ensuring them that acting in accordance with the standard will bring confidence in IT governance of an organization.
- Advising and instructing the organization's governing bodies in IT governance.
- Creating an IT governance dictionary.

Table 2-1 lists the three well-known and vendor-neutral IT governance frameworks, and describes their specifics.

Table 2-1: IT Governance Frameworks

Name of the Framework	Description
IT Infrastructure Library (ITIL) [73]	This framework is accepted worldwide, and is supported by ISO/IEC 20000:2011. The key capabilities of ITIL are support of business outcomes, empowerment of business change, management of risk in accordance with business requirements, optimization of customer experience, etc. The key benefits of ITIL to the organization are reduction of service disruption, improvement of service availability, management of business risks, response to service failures, guarantee that quality of service is equal to the needs and expectations of customers, maximization of return on investment, etc.
Control Objectives for Information and Related Technology (COBIT) [74]	COBIT is a framework developed by the Information Systems Audit and Control Association (ISACA). The newest version of this framework, COBIT 5, is an IT governance and management framework for enterprises. The purpose of this framework is to help managers when dealing with control requirements, technical concerns, and business-related threats. Moreover, regulatory compliance is accentuated; support for increasing the value achieved from IT is provided to companies, and IT governance and control framework implementation is streamlined.
ISO/IEC 27002 [75]	ISO/IEC 27002 standard is used when implementing an ISMS and selecting the controls that are a part of the implementation process. The implementation of a ISMS is based on the previously mentioned standard, ISO/IEC 27001.

2.2.2.2 *Risk Management*

According to ISO 31000:2009 [76], a generic risk management standard, risk is defined as an "effect of uncertainty on objectives", while the effect is defined as a positive or negative departure from the expected outcome. In other words, each objective has a certain level of risk associated with it, which implies that the outcome is uncertain, and can be positive or negative from what is expected. Thus, the uncertainty has to be decreased as much as possible in order to achieve the expected or desired outcome. These uncertainties are a result of organization's internal and external influences, and might be a reason for failing to achieve an objective. Furthermore, ISO 31000:2009 defines risk management as an organized group of actions and procedures that handle organizations' risks that may influence their stated objectives.

Figure 2-9 shows the relationship between the risk management principles, framework, and process. All these concepts will be explained in this section.

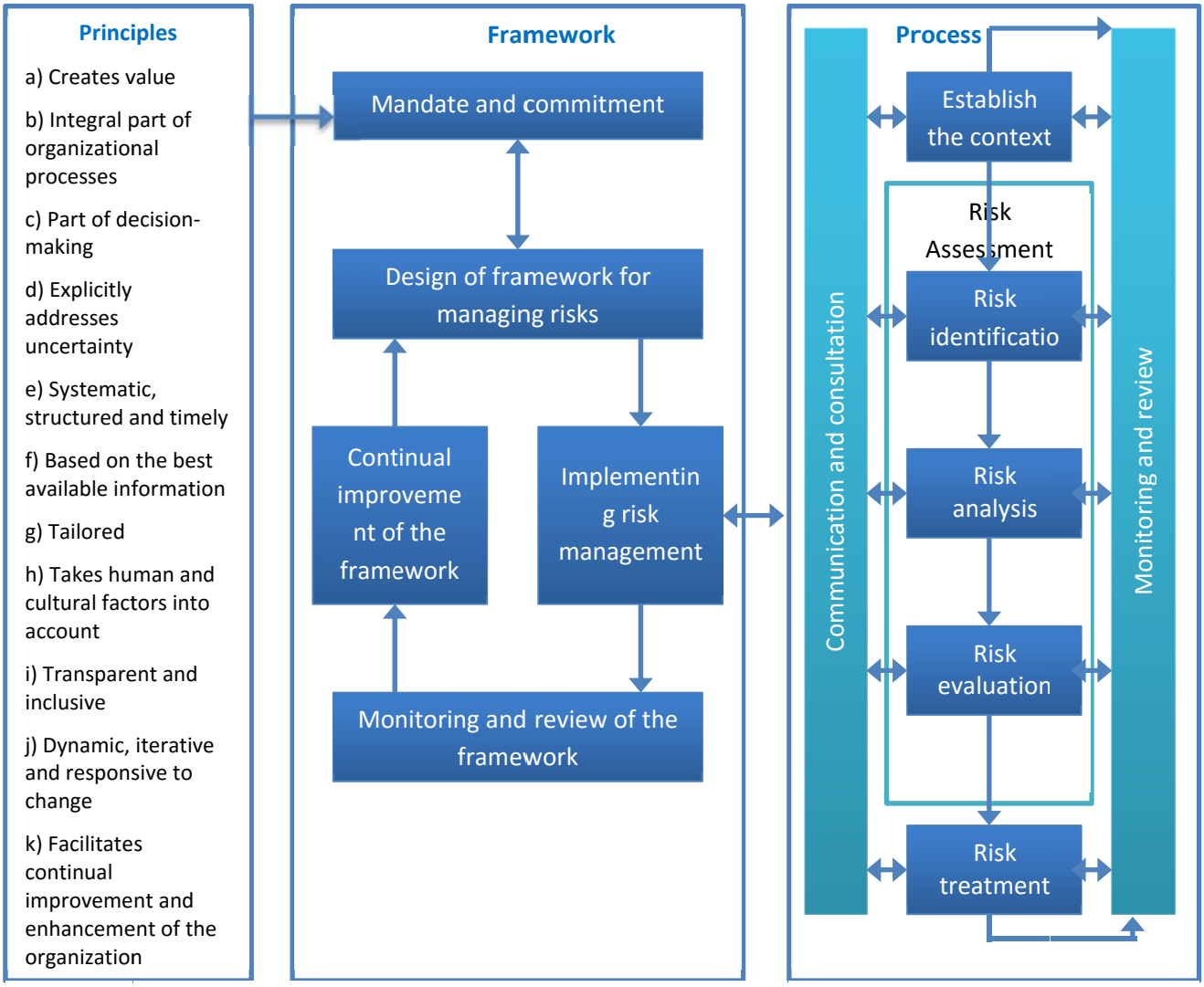

Figure 2-9: Relationships between risk management principles, framework and process (Adapted from Figure 1 of [76])

According to ISO 31000, successful risk management should be based on the following principles:

- Risk management is used to create and defend the value in order to reach an organization's objectives and enhance performance.
- Risk management should be a part of all processes in the organization.
- The process of decision-making should include risk management in order to make better decisions.
- Uncertainties in the organization should be handled with the use of risk management. Thus, the task of risk management is to identify the type and character of uncertainties, and to handle them accordingly.
- A risk management approach should be systematic, structured, and timely in order for risk management to be efficient and dependable.
- The input data used for risk management should be based on the best available information sources.
- Risk management should be tailored to a specific organization and its risk profile.
- Human and cultural factors should be considered when implementing risk management. To be more precise, human skills, objectives, and opinions and their impact on the organization's objectives should be analyzed.
- A risk management approach should be transparent, i.e., open, visible, and available. Moreover, the risk management approach should be inclusive, i.e., all employees involved in the decision making process should be included.
- A risk management approach should be dynamic and responsive to change. In addition, risk management activities should be performed whenever an organization has some objectives to reach.
- Risk management should provide continual improvement and enhancement of an organization.

ISO 31000 also formulated a risk management framework that should be constructed in the following way:

1. Initiate a risk management framework

   Each organization should initiate an efficient risk management framework in order to utilize the risk management process.

2. Mandate and commit to risk management based on the risk management principles

   This step involves several activities, such as stating a risk management policy, determining the values that demonstrate how efficiently an organization is performing risk management activities, expressing objectives, distributing resources, supporting the framework, etc.

3. Design a risk management framework

   A risk management framework is designed with regard to internal and external influences of an organization.

4. Implement a risk management approach

   Implementing a risk management approach consists of implementing a risk management framework and a risk management process.

5. Monitor and review the risk management framework

   It is very important to monitor and review the implemented risk management framework in order to assess its efficiency.

6. Improve the risk management framework

   The implemented risk management framework should be improved based on the feedback from the monitoring and review stage.

Lastly, ISO 31000 defines a risk management process that has a step-by-step nature with some repetitions between the steps. Moreover, the following two steps are continuously applied:

- Communication and consultation

  This step is performed to gather input from the risk management framework, and to provide output for the risk management process.

- Monitoring and review

  The monitoring and review step is important when new risks appear, or already identified risks are modified due to the changes in the organization's objectives.

'*Risk assessment*' is the main part of the risk management process, and is preceded by an '*Establish the context*' step whose aim is to define the internal and external influences that have an impact on the realization of organization's objectives. '*Risk identification*' is the first step of the risk assessment, and it takes as in input the feedback provided by the '*Establish the context*' step. Hence, the goal of the '*Risk identification*' step is to analyze when and how risks can appear. '*Risk identification*' is followed by the '*Risk analysis*' step whose goal is to analyze each risk in terms of the effects that the risk can have on the organization, and probability of the risk's occurrence. '*Risk evaluation*' is the final step in the '*Risk assessment*' process, and its purpose is to determine the risk levels in order to prioritize an organization's risks. 'Risk treatment' is performed after 'Risk assessment' in order to enhance the current controls or implement the new controls. Thus, the goal of this step is to study the risk treatment options of a specific organization, and to choose the most suitable options. As shown in Figure 2-10, the output of the '*Risk treatment*' step serves as an input to the '*Monitoring and review*' step.

According to T. Ackermann [77], risk identification can be performed using numerous techniques that are categorized as collection, creativity, and analytical search techniques. Collection techniques are performed by using checklists or interviews, and are mostly used when identifying previously known risks. Brainstorming and Delphi techniques are a part of creativity techniques, and use divergent thinking as its foundation. In addition, creativity techniques are used when identifying the risks that are unfamiliar to the organization. Attack trees and penetration tests belong to analytical search techniques, and they utilize the present IT infrastructure for risk identification.

2.2.2.3 Compliance

According to ISO 19600:2014 [78], an international standard that provides guidelines on compliance management systems, the term compliance is defined as a result of an organization fulfilling its responsibilities. Furthermore, compliance is inserted into an organization's environment, and this represents a prospect for having a thriving and sustainable organization. ISO also described a compliance management system as a way for an organization to display its dedication to compliance.

IBM states that compliance represents a set of procedures that follow guidelines or instructions that are put in place by government agencies, internal corporate policies or standard groups [79].

However, acting in accordance with compliance requirements is demanding due to the following factors [79]:

- New regulations are regularly being established.
- Some regulations are written unclearly and hence clarification is necessary.
- There is no agreement on the best procedures for compliance.
- There is an overlap between various regulations.
- The already established regulations are changing regularly.

Thus, it can be concluded that compliance is a sustained process because organizations must continuously work in order to meet the compliance requirements relevant to their market.

Table 2-2 lists the two popular compliance legislations and regulations, their geographic coverage, and the compliance requirements stated by those regulations.

Table 2-2: Compliance regulations

Regulation	Geographic coverage	Compliance requirements
Payment Card Industry Data Security Standards (PDI DSS) [80]	International	PDI DSS stated the following compliance requirements: 1. Cardholders' data is protected by installing and supporting a firewall configuration. 2. Security–related parameters should be changed from default settings provided by vendors. 3. Cardholders' data must be protected. 4. The transmission of cardholders' data over public networks must be encrypted. 5. Anti-virus software must be used and updated regularly. 6. Secure systems must be developed and supported. 7. Cardholders' data can be accessed only by businesses that need that data to perform some operation. 8. A unique ID should be given to each user with computer access to its data. 9. Physical access to cardholders' data should be limited. 10. Access to networking assets and cardholders' data should be supervised. 11. Security systems should be frequently examined. 12. A personnel information security policy should be maintained.
Sarbanes-Oxley Act of 2002 [81]	All US companies, and EU companies present in the US	Organizations' internal control efficiency over financial reporting should be supervised. Criminal punishments for security violations and other corporate violations.

According to Microsoft Corporation, *not* complying with the regulations and legislations can have the following consequences [82]:

- The organization's reputation, customer trust, and partner relationships can be lost or damaged.
- Market share of a specific organization will be lost if other organizations in the same sector comply with the regulations.
- Business objectives cannot be reached.
- An organization that does not comply will have financial penalties.
- Credit ratings will decrease.
- Lawsuits against companies are very possible.

2.2.2.4 GRC Framework

The establishment of a GRC framework is to help organizations define their governance and risk objectives, and to state the compliance requirements by using already defined objectives. OCEG has described the elements of a GRC framework in their document called *GRC Capability Model "Red Book"* [63]. Accordingly, a GRC framework is denoted as the GRC Capability Model.

As stated in the *GRC Capability Model "Red Book"*, Principled Performance is defined as a goal of GRC, and it represents an organizations' approach toward achieving their objectives with integrity. Hence, an organization that achieves Principled Performance has various competences, and GRC Capability Model examines these competences. Figure 2-10 shows GRC Capability Model and its components:

Learn This component deals with analyzing the culture, and internal and external context of an organization. In addition, organization's stakeholders are examined in order to state the intentions and approaches of a specific organization.

Align Governance, risk management, and compliance objectives should be aligned with the organization's context and culture.

Perform Objectives, prospects, and threats should be addressed by establishing controls, implementing security policies, educating the organization's personnel, implementing incentives, providing responses, developing communication plans, etc.

Review Efficiency of an organization's activities and controls should be monitored and improved in order to provide assurance to governing authorities and management about the efficiency of achieving the organization's objectives.

OECG's GRC framework is very popular and explains the goals of GRC clearly. Nevertheless, organizations may choose to design and implement their own GRC frameworks in order to match the needs and objectives of their organization precisely.

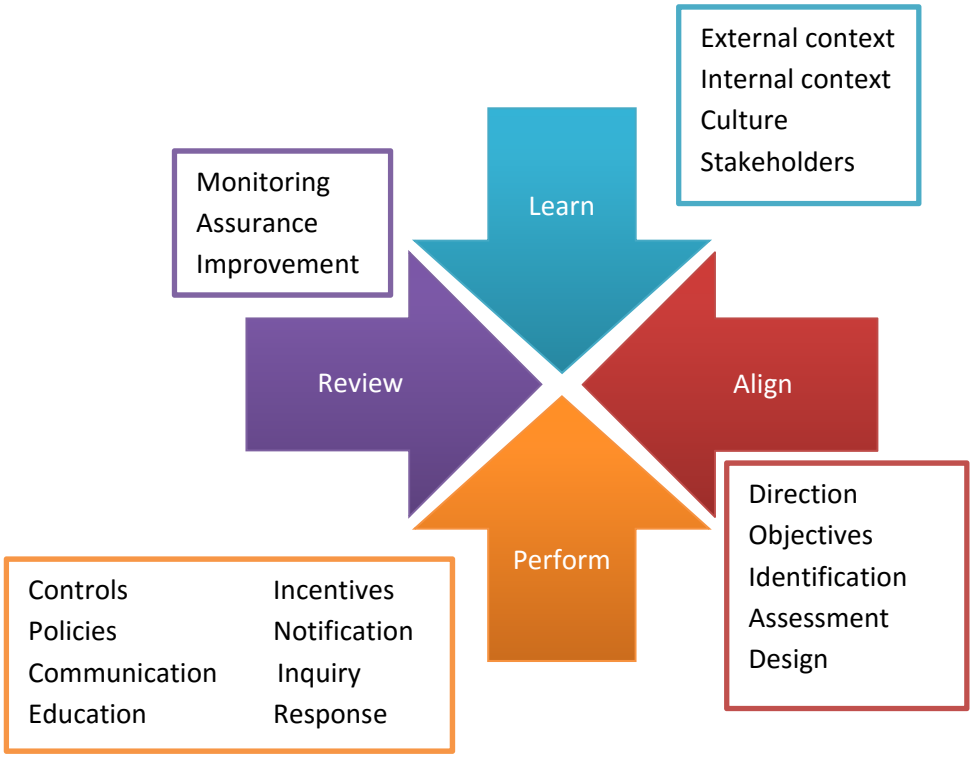

Figure 2-10: GRC Capability Model (Adapted from [63])

2.2.3 Identity and Access Management (IAM)

Identity and access management (IAM) is defined as a security management approach whose aim is to allow authorized users access to certain assets. According to Gartner IT Glossary [83], the objective of IAM solutions is to fulfill progressively demanding compliance requirements. Hence, this security management approach is essential for every organization, and both technical and business skills are needed for developing IAM capabilities. The benefits of implementing an IAM solution are decreased identity management costs and more agile support of business actions.

It is important to first define the core components of IAM, i.e., identity management and access management. According to W. Stallings, IAM is used for handling access to organizations' assets through identity verification to guarantee the identity of a user, and suitable access level determination depending on the verified identity of a user [10]. Identity provisioning is a part of identity management and its responsibility is to give access to verified users or to permit access to users (identity deprovisioning). As stated by E. Osmanoglu in [84], identity management has the following functions:

- Creating distinctive identities and corresponding authentication;
- Inputting the created identities into the selected systems and platforms;
- Identity provisioning and deprovisioning;
- Supervision of identities' data and corresponding credentials;
- Approval of user account creation and modification; and
- Suspension and deletion of user accounts.

Stallings goes on to say that access management deals with providing user authentication and access control services [10]. Moreover, E. Osmanoglu points out in [84] that entitlement management is another name for access management. A group of attributes responsible for denoting user privileges and access rights is known as entitlements. Examples of entitlements are security groups and access rights. A group of functions related to a stated group of access rights is known as roles, and it represents a logical alliance of entitlements. To conclude, access management has the following functions [84]:

- Associating entitlements to roles;
- Changing and deleting entitlements and roles that are appointed to users;
- Allowing the assignment of entitlements and roles to identified users;
- Managing requests for particular entitlements and roles; and
- Reviewing and examining users' history of access.

Figure 2-11 shows the IAM process consists of the following steps [85]:

1. An entity (system user, group of users or automated system) requests access rights.
2. Access request approval process determines if the request triggers a potential segregation of duties conflict by using the segregation of duties rules. Segregation of duties represents an internal control responsible for avoiding deceit by making sure that tasks are divided to various individuals. If it is determined that the request will trigger conflict, a manager or security administrator notifies the application owner of the potential conflict. If there is no indication of a potential conflict, the entity may be granted access rights to the target application or a second level of approval is needed due to the nature of the request.
3. The application owner deals with the second level of approval and those requests that may cause segregation of duties conflicts. The application owner may decide to grant access or route the request to additional approvers.
4. Finally, the target application authenticates the identity of an entity by using entitlement configuration rules.

Figure 2-11 shows an entitlement repository database. This database is a central element of an IAM process. The purpose of this database it to establish, alter, follow, record, and cease the entitlements or access rights associated with entities. Logging software tools are utilized when grouping user accounts based on the functions and controlling user entitlements. Thus, the entitlement repository is responsible for supervising privileges assigned to users, registering submitted access requests and access approvals, storing specific regarding approved access requests and details of the access, etc.

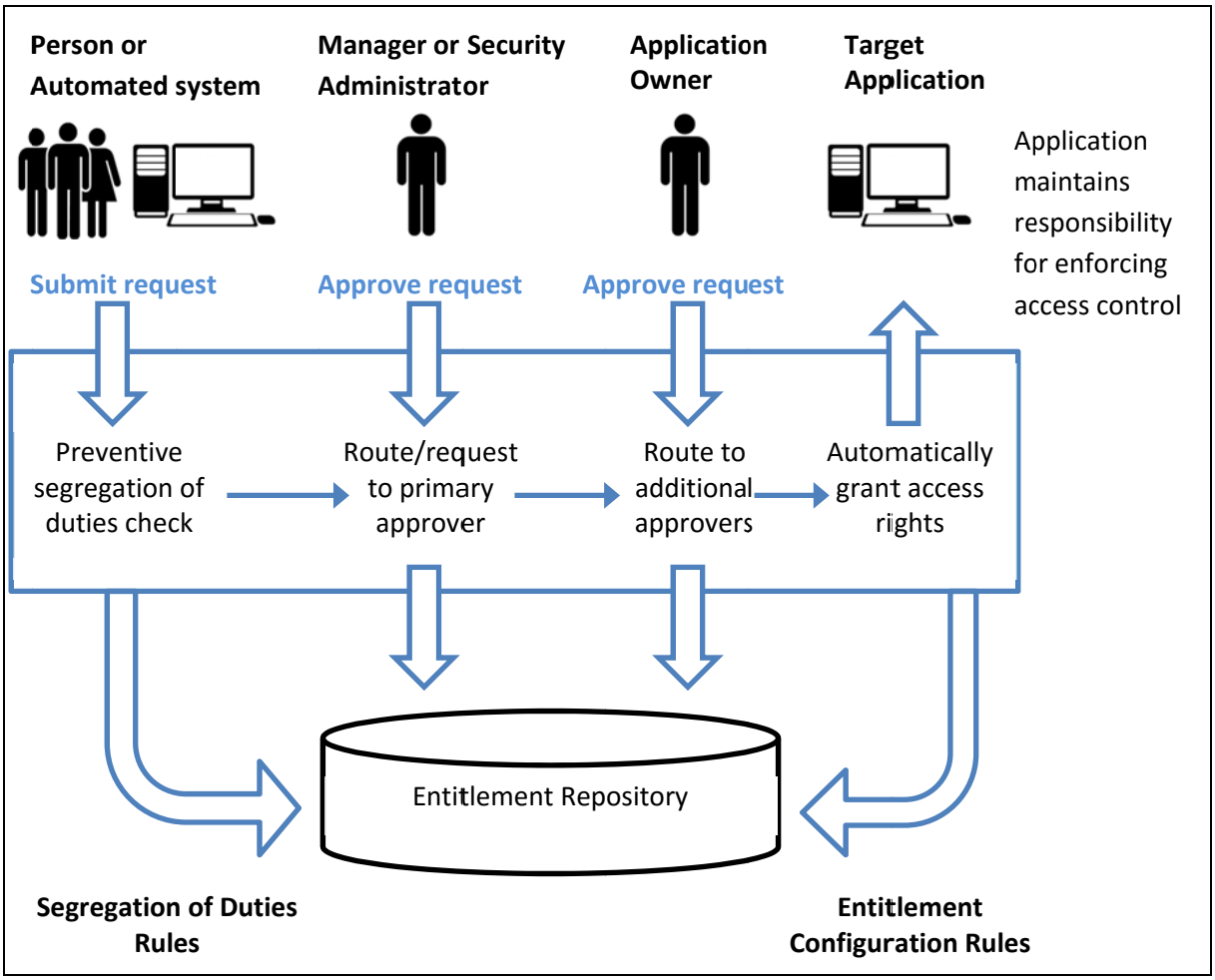

Figure 2-11: IAM Process (Adapted from Exhibit 22.1 of [85])

2.2.3.1 Authentication

According to W. Stallings in [10], authentication represents a method of verifying that the supplied user name corresponds to a correct user. Hence, the purpose of authentication is to decide whether a user or some other entity can access the system resources. As stated by M. Stamp in [86], authentication is an area of access control that answers the following question: "Are you who you say you are?". This section will focus on approaches used when authenticating a user/human to a machine, and some of the approaches to user authentication are the following:

- Username and password

  As W. Stallings has indicated in [10], password systems represent a method of intrusion prevention. All systems that have multiple users accessing their resources demand that users provide both their username and password. The purpose of a password is to authenticate the username of a person that is trying to access system resources. These usernames identify a specific user, for whom the question is does this user have sufficient *authority* to access particular resources, verifying the privileges associated with a specific user, and performing discretionary access control that enables a user to indicate that specific other users are allowed to access this user's files. However, this type of authentication experiences many kinds of attacks, as already mentioned in Section *2.1.4 Security attacks*.

- Biometrics

  As E. Osmanoglu points out in [84], biometrics represents an authentication approach that examines features of a human body that are distinctive to each person and hence can be used for the purpose of authentication. Two types of biometrics methods are physical and behavioral. Physical biometrics analyzes physical features of humans, such as face, voice, retina patterns, fingerprint, etc. In contrast, behavioral biometrics analyzes data obtained from human behaviors. Thus, physical biometrics is static, while behavioral biometrics is dynamic in nature. Osmanoglu also described the following two phases of biometric authentication:

  1. **Enrollment phase**: This phase gathers biometric data about a person, and inserts the data into a specific database. As one might expect, accuracy is very important due to the nature of this stage.
  2. **Recognition phase**: The recognition phase occurs when deciding if a person should be authenticated or not. Therefore, promptness, simplicity, and accuracy are important in this phase.

- Smartcards

  Smartcards incorporate chips that are responsible for storing data and securely performing computations using this data. The difference between smartcards and magnetic stripe cards is that the chips incorporated in smartcards are more secure as they can perform secure processing on the data, while magnetic strip cards do not perform any processing and their data can be read by any magnetic strip card reader. Smartcards are usually used for passports, ID cards, cellular phone subscriber identification modules, and increasingly for credit/debit cards.

- Personal Identification Number (PIN)

  A password that generally consists of digits is known as personal identification number (PIN), and it is mostly used when performing authentication for payment cards and for authenticating access to a subscriber identification module. According to Robert J. Bartz in [87], ISO permits the length of a PIN to be from four to twelve digits, but the usual length is four digits.

- Digital certificates

  A digital certificate or public key certificate is a document that is signed by a trusted third party, usually a certificate authority (CA). A digital certificate is used for authentication purposes. As stated in Ertem Osmanoglu's book *Identity and Access Management: Business Performance Through Connected Intelligence* [84], a public key infrastructure (PKI) is generally used to bind a public key of an entity to its identity.

2.2.3.2 Authorization

As stated in William Stallings' book *Network Security Essentials: Applications and Standards* [10], authorization is a method of permitting access to particular system resources. Hence, authorization is performed after authenticating an entity. According to M. Stamp in [86], authentication is an area of access control that answers the following question: "Are you allowed to do that?".

An example of performing authorization is using an access matrix defined by Butler W. Lampson [88]. This access matrix is used when deciding which system resources a particular user can access. This concept has three main elements: *objects* denoted by X that represent system resources (domains, files, processes, segments, etc.) that need access protection, *domains* denoted by D that represent entities that have been authenticated and can have access to particular objects, and *access matrix* denoted by A. Figure 2-12 shows a portion of an access matrix with rows representing domain names, and columns representing object names. A[i, j] is an element of the

access matrix, and it indicates which kind of access domain *i* has to object *j*. The values of matrix elements are denoted as *access attributes*, and the most common values are: read, write, and wakeup. Every access attribute has a *copy flag bit* attached to it, and an asterisk is used to denote that a copy flag bit is set. The purpose of the copy flag bit is to supervise the transfer of access rights. If the access attribute has the copy flag bit set, then an object in a domain can copy their access rights to other fields in the same column (same object).

	Domain 1	Domain 2	Domain 3	File 1	File 2	Process 1
Domain 1	*owner control	*owner control	*call	*owner *read *write		
Domain 2			call	*read	write	wakeup
Domain 3			owner control	read	*owner	

Figure 2-12: Access matrix (Adapted from Figure 1 of [88])

Figure 2-13 shows a simplified authentication and authorization process.

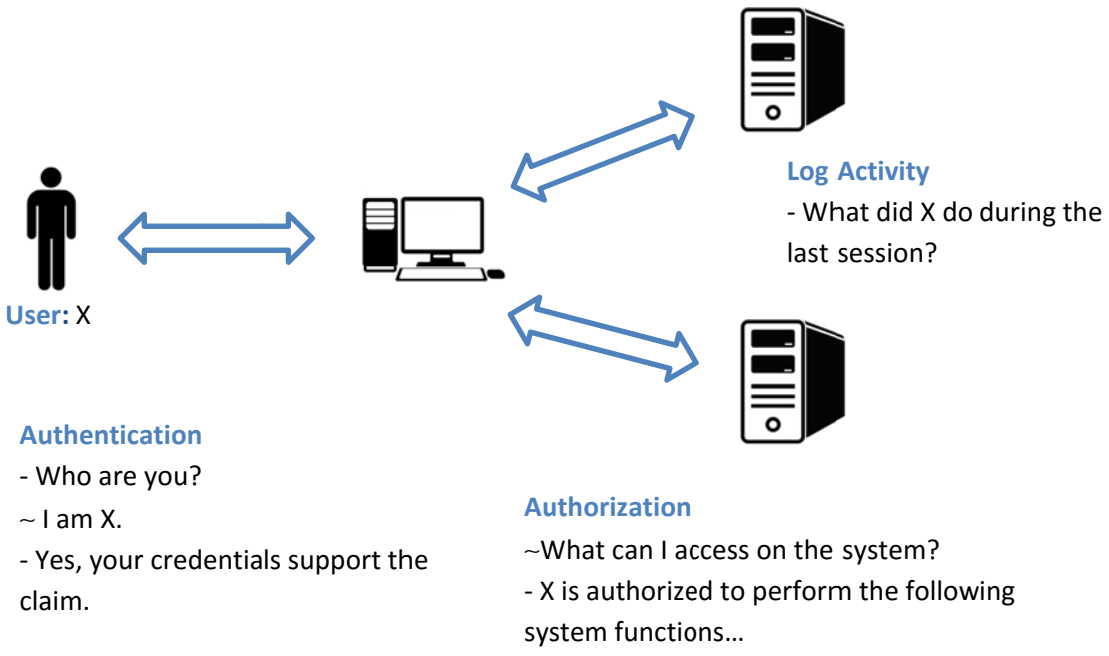

Figure 2-13: Authentication and authorization process (Adapted from Exhibit 22.2 of [85])

2.3 Summary

This chapter introduced the reader to various concepts that are essential to understand the following chapters. Information security and information security management concepts and principles were discussed in order to understand the security management approaches that were also analyzed in this chapter.

3 Methodology

The purpose of this chapter is to provide an overview of the research method used in this thesis. The empirical model was used in order to gain knowledge by means of direct and indirect observation or experience. The type of the research and time available to conduct this project were considered when choosing an appropriate methodology.

Section 3.1 describes the research process. Section 3.2 details Gartner Inc.'s methodology [4] used when they producing Gartner Magic Quadrants [3]. Section 3.3 focuses on market research for SIEM solutions. Section 3.4 concentrates on market research for the following GRC segments: IT Risk Managements, Operational Risk Management, and IT Vendor Risk Management solutions. Section 3.5 focuses on IAM solutions. Section 3.6 draws conclusions regarding all of the analyzed quadrants. Section 3.7 discusses the reliability and validity of the data collected.

The goal of this chapter is to present the solutions that are currently available in the market for the security management approaches described in Chapter 2. The goal is to identify the two leading security management solutions.

3.1 Research Process

This research process focuses on performing market research for three security management approaches: SIEM, IAM, and GRC. The outcome of this process is the identification of security management leaders in order to select the solution that is most suitable for Swedish Armed Forces. Figure 3-1 shows the steps conducted in order to carry out this research.

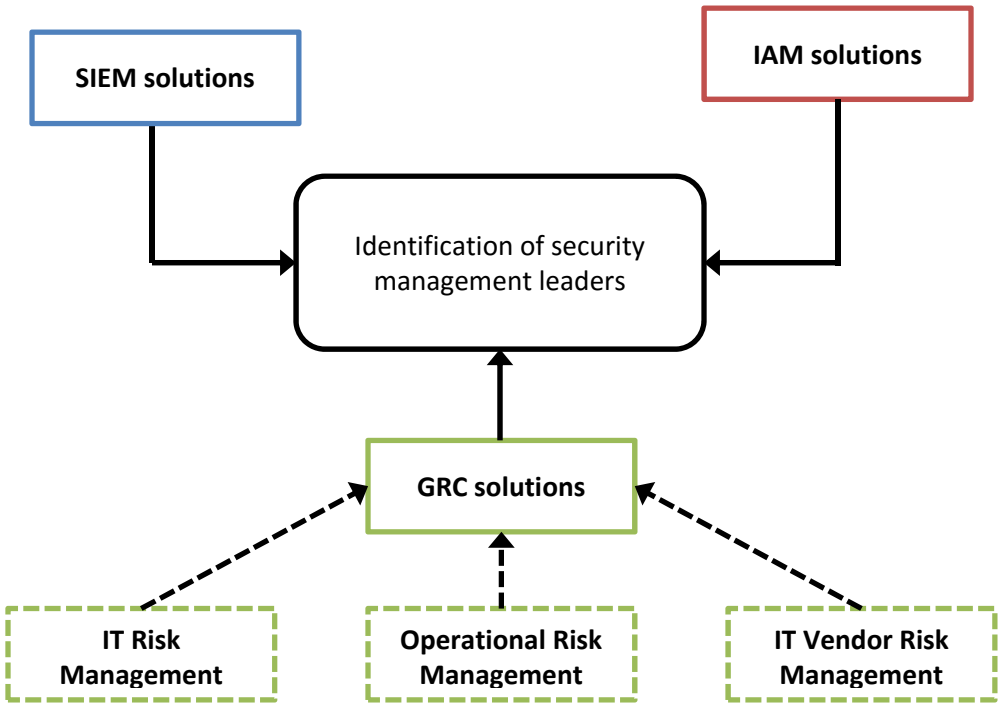

Figure 3-1: Research Process

3.2 Gartner's Magic Quadrant Research Methodology

Gartner, Inc. has developed a very organized methodology used for performing Gartner Magic Quadrant analysis. As stated by D. Black and J. Thomas in [89], Gartner, Inc.'s analysts, Magic Quadrants reports provide an extensive analysis of a specific market and those vendors that operate in that market. Understanding these reports is important when selecting a particular solution based upon these reports.

Figure 3-2 shows the Magic Quadrant graph that has the following two axes:

- **Ability to execute:** Vendors' product offer, financial growth, alertness to market changes, product development, marketing implementation, customer experience, and ability to meet the objectives are considered when analyzing the ability to execute.
- **Completeness of vision:** Vendors' perception of a market, business model, innovative aspects, marketing approach, sales scheme, product development approach, industry approach, and geographic strategy are considered when analyzing the completeness of vision.

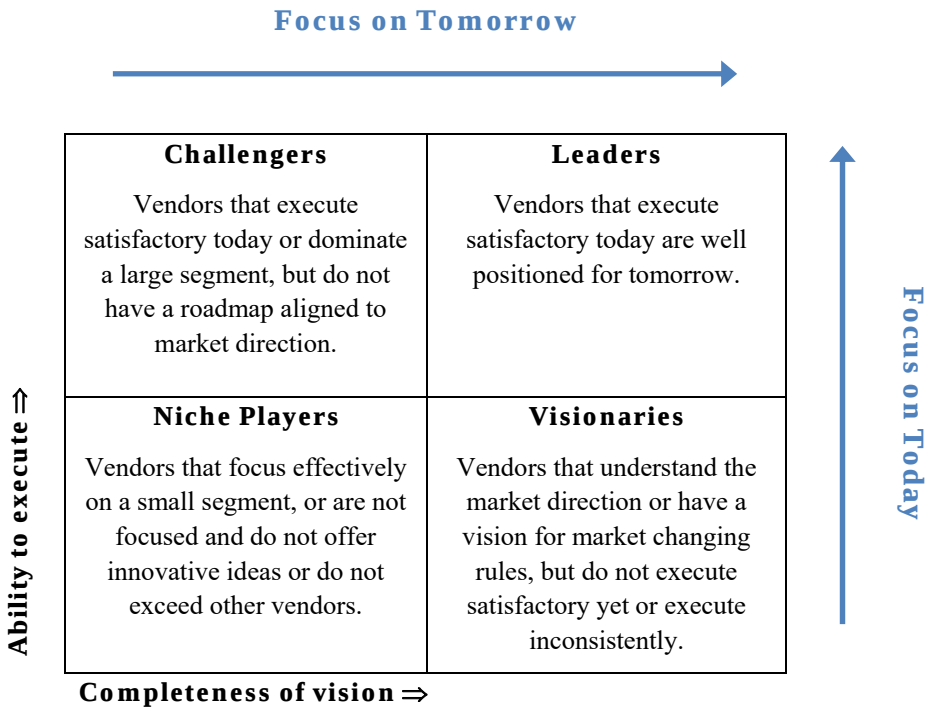

Figure 3-2: The Magic Quadrant (Adapted from Figure 1 of [89])

Gartner, Inc.'s Magic Quadrants classify technology vendors according to the following four categories [89]:

- Leaders

  Vendors that provide fully developed solutions that fulfill the market requirements and are characterized as promising to maintain their established market position are classified as leaders. Leaders' distinctive features are significant emphasis and investment in their solutions, which led them to becoming leaders, and having an influence on the market direction. Naturally, leaders have many pleased customers and a significant financial gain.

- Visionaries

  Vendors that follow and understand the market direction, but did not entirely fulfill the market requirements are classified as visionaries. Visionaries' distinctive feature is innovation; they frequently present new features and services. However, they have not established financial stability and their sales & distribution channels have yet to be built. If companies welcome their innovative features or they establish new partnerships, then visionaries may become leaders or challengers.

- Challengers

  Vendors that have a high ability to execute, but low completeness of vision are classified as challengers. Challengers' distinctive features are a weak vision, non-innovation, and lack of comprehension of market direction. If their vision matures, then challengers can improve to becoming leaders.

- Niche Players

  Vendors that have both low ability to execute and limited completeness of vision are niche players. However, they might be successful in some market sector. Niche players' distinctive features are focusing on a particular geographic area or some range of capabilities. Additionally, new vendors are most often classified as niche players. Hence, niche players do not have many customers and their vision needs to develop. Analyzing niche players is very difficult because some vendors are new and their vision and offering may develop, while some other vendors might not be new but are simply not following the market's direction.

Although leaders have both high ability to execute and completeness of vision, this does **not** indicate that these leaders' solutions are the best choice for every client. Hence, other vendors should not be overlooked and meeting a given organization's needs should be the priority.

3.3 SIEM Market Research

This section presents Magic Quadrant for SIEM. According to Gartner, Inc.'s Magic Quadrant report for SIEM for the year 2015 [90], vendors had to satisfy the following requirements in order to be a part of the Magic Quadrant for the year 2015:

- Vendors' solutions *must* include both SIM and SEM functionalities.
- Vendors' solutions *must* capture data from wide-ranging sources (networking devices, security devices, servers, security programs, etc.).
- End-user organizations provide assessment lists regarding SIEM solutions, and vendors that are not on these lists will *not* be included in Magic Quadrant.
- Clients must receive solutions as a software or application program, and *not* as a service.
- Vendors' solutions *cannot* offer SIEM functions that are focused on data from their own solutions.
- Vendors' income for their SIEM solutions *must* be over $13.5 million per year.

Gartner, Inc.'s Magic Quadrant report also stated that the evaluation criteria was divided into the following two categories [90]:

1. Ability to execute
   - **Product offer**: Vendors' solutions should support sectors such as security monitoring, security analytics, compliance reporting, etc.

- **Financial growth**: Vendors' financial status is analyzed in order to determine whether the vendors can invest in new SIEM features of their solutions.
- **Sales accomplishment**: This criterion deals with analyzing the financial aspect of vendors' SIEM solutions.
- **Alertness to market changes**: Response to market changes is very important in order for a solution to remain relevant.
- **Marketing implementation**: Vendors' marketing strategy is analyzed, and variations as a result of different industries and geographical regions are also examined.
- **Customer experience**: Customer experience is evaluated by using qualitative interviews and feedbacks from clients. The evaluation focuses on the solution's deployment difficulty, support, ability to be expanded, operation, etc.
- **Ability to meet the objectives**: This criterion evaluates the solutions' ability to meet the organizations' objectives.

2. Completeness of vision

- **Vendor's perception of a market**: It is important to analyze whether a certain vendor understands the market needs, and hence responds to the needs by including new functionalities in its solution.
- **Marketing approach**: Vendor's skill to present its solution and differences that make that solution stand out is also very important.
- **Sales scheme**: Sales scheme analyzes vendors' approach to selling their product.
- **Product development approach**: This criterion evaluates approach to product development. Thus, it evaluated whether solutions satisfy the newest SIM and SEM requirements.
- **Industry strategy**: Industry strategy investigates whether a particular vendor is adjusting its SIEM functionalities according to the different industries.
- **Geographic strategy**: Geography strategy investigates whether a particular vendor is adjusting its SIEM functionalities according to the different geographical regions.
- **Innovative aspects:** This criterion evaluates the innovativeness of SIEM solutions when meeting customer needs.

Figure 3-3 shows the following classification of vendors:

- **Leaders**: IBM Security, Splunk, HP, Intel Security, LogRhythm
- **Visionaries**: AlienVault, EMC (RSA)
- **Niche Players**: Trustwave, Micro Focus (NetIQ), SolarWinds, AccelOps, EventTracker, BlackStratus

It can be concluded by looking at the Magic Quadrant for SIEM that IBM Security is a definite leader due to having the highest ability to execute and completeness of vision. What is more, IBM Security was also the leader for year 2014, which indicates that this vendor is constantly investing in its solution. It is interesting to note that categories Challengers and Visionaries both have only one solution, while Leaders and Niche players have several solutions.

Figure 3-3: Magic Quadrant for SIEM (Adapted from Figure 1 of [90])

3.4 GRC Market Research

As already mentioned in section 2.2.2, Gartner, Inc.'s OneGRC research program that is responsible for evaluating GRC market and its segments has defined the several market segments within GRC and hence each of those segments has Magic Quadrant associated to it. This section will analyze the following market segments: IT Risk Management, Operational Risk Management, and IT Vendor Risk Management.

3.4.1 IT Risk Management

This section presents Magic Quadrant for IT Risk Management. According to Gartner, Inc.'s Magic Quadrant report for IT Risk Management for the year 2015 [91], vendors had to satisfy the following requirements in order to be a part of the Magic Quadrant for the year 2015:

- Vendors' solutions *must* focus on at the minimum four out of the following five functions and work flows:
    1. Policy management
    2. Compliance reporting

3. Security operations evaluation and reporting
4. IT risk assessment
5. Incident management

- Vendors' solutions *must* use a single and integrated software platform.
- Vendors' income for their IT Risk Management solutions *must* be no less than $3 million per year.

Gartner, Inc.'s Magic Quadrant report for IT Risk Management also discussed the evaluation criteria that are the same as for SIEM solutions in the previous section. Figure 3-4 shows the following classification of vendors:

- **Leaders**: EMC (RSA), IBM Security, MetricStream
- **Visionaries**: Module, Rsam, Agiliance, LockPath
- **Challengers**: Nasdaq
- **Niche Players**: Allgress, ControlCase, Brinqa

It can be concluded by looking at the Magic Quadrant for IT Risk Management that IBM Security is also a leader in this security management approach, and is the only leader from the SIEM Magic Quadrant that is also a leader in this quadrant. EMC (RSA) has the highest ability to execute, while IBM Security has the highest completeness of vision. Module is an example of a vendor who could become a leader if more effort was put into their service delivery.

Figure 3-4: Magic Quadrant for IT Risk Management (Adapted from Figure 1 of [91])

3.4.2 Operational Risk Management

This section presents Magic Quadrant for Operational Risk Management. According to Gartner, Inc.'s Magic Quadrant report for Operational Risk Management for the year 2015 [92], vendors had to satisfy the following requirements in order to be a part of the Magic Quadrant for the year 2015:

- Vendors' solutions *must* focus on a minimum of four out of the following five critical capabilities:
    1. Risk and control assessment
    2. Incident management
    3. Risk mitigation
    4. Key risk indicators monitoring
    5. Risk quantification
- Vendors' income for their Operational Risk Management solutions *must* be no less than $6 million per year.

Gartner, Inc.'s Magic Quadrant report for Operational Risk Management also discussed the evaluation criteria that are the same as for SIEM solutions. Figure 3-5 shows the following classification of vendors:

- **Leaders**: IBM Security, EMC (RSA), MetricStream, Nasdaq, Thomson Reuters, SAS
- **Visionaries:** Enablon, Modulo, Covalent
- **Challengers**: Protiviti, SAP
- **Niche Players**: Wolters Kluwer, Riskonnect

Figure 3-5: Magic Quadrant for Operational Risk Management (Adapted from Figure 1 of [92])

It can be concluded by looking at the Magic Quadrant for Operational Risk Management that the majority of vendors, who satisfied the requirements for being a part of Magic Quadrant, are classified as leaders. IBM Security, EMC (RSA), and MetricStream are leaders again. Nasdaq, who is challenger in Magic Quadrant for IT Risk Management, is a leader in this quadrant. It is interesting that SAS and Thomson Reuters are leaders in this GRC segment but are not included in Magic Quadrant for IT Risk Management. Modulo is classified as a visionary for both IT Risk Management and Operational Risk Management. Overall, vendors who were leaders in previous quadrants are also leaders in this one, which indicates that the quality of their solutions is very satisfactory.

3.4.3 IT Vendor Risk Management

Magic Quadrant for IT Vendor Risk Management will be presented in this section. According to Gartner, Inc.'s Magic Quadrant report for IT Vendor Risk Management [93] that was released in December of 2014, vendors had to satisfy the following requirements in order to be a part of the Magic Quadrant:

- Vendors' solutions *must* be implemented for at least 15 clients.
- Vendors' solutions *must* have a high probability of customer increase in the following three years.
- Vendors' income for their IT Vendor Risk Management solutions *must* be no less than $1 million per year.
- Vendors' solutions *cannot* concentrate on non-IT third-party risk management.
- Vendors' solutions *cannot* offer predominantly vendor risk management services instead of a software solution.

Gartner, Inc.'s Magic Quadrant report for Operational Risk Management also discussed the evaluation criteria that are the same as for SIEM solutions.

Figure 3-6 shows the following classification of vendors:

- **Leaders**: EMC (RSA), MetricStream
- **Visionaries**: Prevalent
- **Challengers**: Modulo, Rsam, Quantivate, Agiliance
- **Niche Players**: LockPath, Brinqa, Allgress

It can be concluded by looking at the Magic Quadrant for Operational Risk Management that EMC (RSA) and MetricStream are leaders in this GRC sectors as well. Rsam, Agiliance, and Modulo were visionaries in the previous segments, but are challengers in this one. LockPath is a niche player in this segment and visionary in IT Risk Management, while Brinqa and Allgress are niche players in both of them. Prevalent and Quantitative appear for the first time.

Figure 3-6: **Magic Quadrant for IT Vendor Risk Management (Adapted from Figure 1 of [93])**

3.5 IAM Market Research

Gartner, Inc. does not produce a Magic Quadrant report for IAM, but does produce a report for Identity Governance and Administration (IGA), the term was established by Gartner, Inc. in 2013. IGA actually represents an IAM solution that is responsible for identity administration, identity governance, and a study of combining them into one platform. According to F. Gaehtgens and B. Iverson, IGA is responsible for the following functionalities [94]:

- Supporting digital identities
- Management of entitlements
- Management of access requests
- Coordinating tasks to support functions such as access approvals, notifications, etc.
- Access certification
- Password management
- Audit management
- Providing reports

Magic Quadrant for IGA will be presented in this section. According to Gartner, Inc.'s Magic Quadrant report for IGA [93] that was released in January of 2015, vendors had to satisfy the following requirements in order to be a part of the Magic Quadrant:

- Vendors' solutions *must* provide user interfaces that support multiple user profiles.
- Vendors' solutions *must* support identity and entitlement life cycles.
- Vendors' solutions *must* support entitlement discovery.
- Vendors' solutions *must* support role discovery.
- Vendors' solutions *must* provide functionalities for creation and editing of identity and access data.
- Vendors' solutions *must* provide certification tools.
- Vendors' solutions *must* support password management and synchronization amongst various target systems.
- Vendors' solutions *must* support auditing and compliance.
- Vendors' solutions *must* support entitlement management and administration.
- Vendors' solutions *must* support role management and administration.
- Vendors' solutions *must* support enforcement of identity and access policies.
- Vendors' solutions *must* provide logging functionalities.
- Vendors' solutions *must* support reporting and analytics.

Gartner, Inc.'s Magic Quadrant report for IGA also discussed the evaluation criteria that are the same as for SIEM solutions.

Figure 3-7 shows the following classification of vendors:

- **Leaders**: SailPoint, IBM Security, EMC (RSA), Oracle, Courion
- **Visionaries**: CA Technologies
- **Challengers**: Dell, NetIQ, Hitachi ID Systems
- **Niche Players**: Beta Systems, AlertEnterprise, Omada, SAP, Evidian, Fischer International, Avatier, The Dot Net Factory, Atos, Identity Automation

It can be concluded by looking at the Magic Quadrant for IGA that SailPoint is a definite leader due to them having the highest ability to execute and greatest completeness of vision. EMA (RSA) and IBM Security are leaders in this segment as well. Leaders that appear for the first time are Oracle and Courion. Some vendors, such as Dell, NetIQ, AlertEnterprise, etc. are close to moving to a new category if they improved their completeness of vision or ability to execute.

Figure 3-7: Magic Quadrant for IGA Management (Adapted from Figure 1 of [94])

3.6 Magic Quadrant Conclusions

The previous sections analyzed five Magic Quadrant reports in order to become familiar with the positioning of vendors. The Swedish Armed Forces store a lot of sensitive information that needs strong protection in order to avoid any security incidents. Thus, a strong security management solution is needed for such an organization. Although all of the categories in the Magic Quadrant should be regarded and not just the leaders, the best solution for Swedish Armed Forces is surely the one provided by a leading vendor.

Table 3-1 summarizes the findings from previous sections. It is evident that IBM Security and EMC (RSA) are very successful vendors that offer many different security management approaches and both have excellent positioning. Hence, the following chapter will present the details regarding IBM Security and EMC (RSA) solutions. A solution that satisfies the most requirements as stated by Swedish Armed Forces will be selected and modified in order to satisfy the full set of requirements.

Table 3-1: Magic Quadrant Summary

Magic Quadrant	Leaders	Visionaries	Challengers	Niche Players
SIEM	IBM Security, Splunk, HP, Intel Security, LogRhythm	AlienVault	EMC (RSA)	Trustwave, Micro Focus (NetIQ), SolarWinds, AccelOps, EventTracker, BlackStratus
IT Risk Management	EMC (RSA), IBM Security, MetricStream	Module, Rsam, Agiliance, LockPath	Nasdaq	Allgress, ControlCase, Brinqa
Organizational Risk Management	IBM Security, EMC (RSA), MetricStream, Nasdaq, Thomson Reuters, SAS	Enablon, Modulo, Covalent	Protiviti, SAP	Wolters Kluwer, Riskonnect
IT Vendor Risk Management	EMC (RSA) MetricStream	Prevalent	Modulo, Rsam, Quantivate, Agiliance	LockPath, Brinqa, Allgress
IGA	SailPoint, IBM Security, EMC (RSA), Oracle, Courion	CA Technologies	Dell, NetIQ, Hitachi ID Systems	Beta Systems, AlertEnterprise, Omada, SAP, Evidian, Fischer International, Avatier, The Dot Net Factory, Atos, Identity Automation

3.7 Assessing reliability and validity of the data collected

This section explains why the conclusions that were made in the previous sections are both reliable and valid. The following factors have contributed to their reliability and validity:

- Gartner, Inc.'s Magic Quadrants for many years represented the most influential source of vendor information.
- The research methodology deployed by Gartner, Inc. is very structured and comprehensive. Gartner, Inc.'s analysts analyze both the features of each solution and customer reviews that are very valuable when rating solutions.
- The Magic Quadrants that were analyzed are up-to-date.
- The analysis covered three security management approaches, SIEM, GRC and IAM, along with their segments.
- The top leaders, IBM Security and EMC (RSA), were selected based on their positions in all of the security management approaches that were analyzed.

3.8 Summary

This chapter introduced the reader to Gartner, Inc.'s research methodology that was employed when producing their Magic Quadrants reports. Moreover, the Magic Quadrants reports for SIEM, GRC, and IAM were presented and discussed. Finally, two leaders, IBM Security and EMC (RSA), were selected based on these reports.

4 Security Management Leaders

The purpose of this chapter is to present solutions developed by two leaders in the field of security management. These leading vendors are IBM and EMC (RSA), and they were selected based on the security management market research that was performed in the previous chapter. Thus, the goal is to analyze the solutions provided by these vendors.

Section 4.1 presents IBM InfoSphere Guardium. Section 4.2 introduces RSA Archer. Section 4.3 summarizes the findings from Sections 4.1 and 4.2.

4.1 IBM InfoSphere Guardium

IBM InfoSphere Guardium or IBM Security Guardium is an extensive data security platform developed by IBM Security. The purpose of IBM InfoSphere Guardium is to protect sensitive data that is stored in various locations, such as cloud, databases, file systems, etc. In addition, this platform also provides an automated risk analysis that is employed for discovering organizations' internal and external risks.

According to Whei-Jen Chen, et al., the IBM InfoSphere architecture components are categorized as follows [95]:

1. **Appliances**: This category consists of the following subcategories:
    - *Collectors* are responsible for recording and evaluating the database activity.
    - *Aggregators* are in charge of gathering the data from collectors, and making reports based on the data gathered from various collectors.
    - *Central Managers* are responsible for handling and monitoring of several appliances.
2. **Agents**: Agents are installed on the database server. This category consists of the following subcategories:
    - *S-TAP (Software-Tape)* agent is in charge of observing the activities, and transferring those observations to the collector.
    - A *Guardium Installation Manager* agent is responsible for enabling the installation, updating, and configuration alteration of agents.
    - A *change Audit System* agent records changes made in audit information of configuration files that are stored on the database server.
    - An *Instance Discovery* agent is in charge of acquiring information from databases, ports, etc.

IBM Security states that IBM InfoSphere Guardium has the following capabilities [96]:

- Discovery and classification of sensitive data;
- Automatic discovery of compliance risks;
- Monitoring of user activities within databases, files, etc.
- Discovery and correction of risks by evaluating data usage behaviors with the use of machine learning and progressive analytics;
- Evaluation and scanning of audit data in order to discover internal or external database attacks by using a Threat Diagnostic Center;
- Investigation of organizations' data security by using a Data Protection Dashboard;

- Automated data compliance and auditing capabilities are provided in order to protect organizations from legal responsibilities;
- Protection of critical data by using encryption techniques, data masking, data redaction, etc.
- Access management is provided in order to avoid suspicious activities;
- Support of both conventional and latest data technologies;
- Reduction of organizations' costs; and
- Enhancement of organizations' results.

Moreover, IBM InfoSphere Guardium supports the following use cases:

1. IBM InfoSphere Guardium Data Activity Monitor

   The purpose of this use case is to block illegal data access, aids in guaranteeing data integrity, provides automated compliance controls, and defends against threats. As stated by IBM, this use case provides the following functionalities [97]:

   - Protection of sensitive data by discovering internal and external risks;
   - Monitoring and auditing of data activity for every data platform and protocol;
   - Real-time enforcement of security policies for all data access and activities performed by users;
   - Construction of a unified and normalized audit data repository for organizations' compliance, forensics, and reporting;
   - Support for various data environments (databases, data warehouses, etc.); and
   - Support for prompt data environment changes.

2. IBM InfoSphere Guardium Activity Monitor for Files

   The goal of this use case is to manage access to files that need to be protected. According to IBM, this use case provides the following functionalities [98]:

   - Monitoring and auditing of *file* data activity within organizations' file systems.
   - Real-time enforcement of security policies for all file access and activities performed by users;
   - Construction of a unified audit data repository for organizations' compliance, forensics, and reporting; and
   - Support for various data environments (platforms, file systems, OSs).

3. IBM InfoSphere Guardium Data Redaction

   Information governance utilizes this use case for protecting sensitive data from accidental release. Hence, sensitive data is identified and removed from documents that are shared to everyone. IBM Security states that this use case provides the following functionalities [99]:

   - Protection against unintentionally releasing sensitive data;
   - Transformation of slow and non-automatic redaction activities into automated redaction procedures;
   - Support for regulatory compliance by employing data governance; and

- Provision of reporting procedures.

4. IBM InfoSphere Guardium Vulnerability Assessment

   The purpose of this use case is to identify susceptibilities by scanning data infrastructures, such as databases, data warehouses, etc. In addition, IBM InfoSphere Guardium Vulnerability Assessment also recommends restorative activities. This use case has the following capabilities [100]:

   - Detection of data sources;
   - Grouping of sensitive data;
   - Observing of entitlements and credentials belonging to data sources;
   - Support for automated scanning of susceptibilities;
   - Support for behavioral evaluations;
   - Provides access to various susceptibility tests; and
   - Provision of reporting procedures related to vulnerability assessment.

5. IBM InfoSphere Guardium Express Activity Monitor for Databases

   Distributed database repositories require secure data activity monitoring and this is performed by IBM InfoSphere Guardium Express Activity Monitor for Databases. In addition, this use case provides real-time alerts and audit logs that are used for compliance reports. IBM Security states that IBM InfoSphere Guardium Express Activity Monitor for Databases has the following capabilities [101]:

   - Discovery and classification of sensitive data;
   - Provides efficient compliance by using policies, reports, etc.;
   - Real-time monitoring and auditing of database activity; and
   - Development of organizations' functionalities and operations.

6. IBM InfoSphere Guardium Data Encryption

   This use case uses encryption techniques to protect the sensitive data in order to fulfill compliance requirements. The following capabilities are offered to clients [102]:

   - Policy management is used to streamline an organizations' security management; and
   - Provides compliance capabilities in order to meet governance and compliance requirements.

4.2 RSA Archer

EMC (RSA) RSA Archer is a platform responsible for managing risks. This platform supports the following use cases:

1. RSA Archer IT & Security Risk Management

   According to RSA, this use case provides IT and security risk management to organizations, and has the following capabilities [103]:

- Creation of a controls framework by with the aid of an information security policy framework, which consists of policies, standards, guidelines, and procedures;
- Association of controls with an organization's objectives;
- Management of the development of policies;
- Performance evaluation and reporting;
- Test automation and controls monitoring;
- Management of compliance matters;
- Ranking of IT and security risks;
- Data scanning in order to identify susceptibilities;
- Monitoring of IT and security risks;
- Management of risks and threats evaluations;
- Management of concerns that emerged through risk-related procedures; and
- Implementation and documentation of incident response procedures.

2. RSA Archer Enterprise & Operational Risk Management

   RSA Archer Enterprise & Operational Risk Management gathers risk-related information in order to recognize, evaluate, handle, and observer enterprise and operational risks. Hence, some of the capabilities of this solution are the following [104]:

   - Creation of a risk management classification;
   - Classification of risks;
   - Implementation of risk evaluations;
   - Loss events handling and reporting;
   - Recording of business procedures;
   - Enlargement of operational risk platform; and
   - Management of main risk pointers.

3. RSA Archer Regulatory and Corporate Compliance

   This solution helps organizations to fulfill compliance requirements by performing the following activities [105]:

   - Creation of information storage system for managing governance;
   - Response to regulatory change by investigating the effects of regulations on controls and policies, and identifying concerns and breaches; and
   - Management of assurance and compliance by handling procedures and controls, and ensuring compliance reporting.

4. RSA Archer Audit Management

   According to RSA (EMC), some of the capabilities of RSA Archer Audit Management are the following [106]:

   - Formation of risk and compliance corporate structure and responsibility;
   - Identification and allocation of duties for handling breaches, concerns, and faults;

- Documentation of audit arrangements;
- Management of audit arrangements;
- Support of an efficient audit reporting;
- Development and supervision of audit plans; and
- Execution of audit quality assurance processes.

5. RSA Archer Business Resiliency

   RSA Archer Business Resiliency helps organizations to minimize the effect of problems that interrupt organizations' activities and processes, and emergency incidents. Some of the capabilities of this solution are the following [107]:

   - Incident management by forming organization's corporate structure and using accountability across these structures;
   - Handling of incident management lifecycle;
   - Risk assessment;
   - Business impact evaluation;
   - Identification of organization's crucial processes;
   - Documentation of business continuity plans;
   - Formation of IT disaster recovery plans;
   - Handling and recording of crisis events;
   - Business continuity plans testing; and
   - IT disaster recovery plans testing.

6. RSA Archer GRC Platform

   RSA Archer GRC Platform has the following capabilities [108]:

   - Automation of an organizations' processes;
   - Improvement of workflow efficiency and effectiveness;
   - Access control;
   - Real-time reporting;
   - Management of organizations' risks, policies, weaknesses, etc.
   - Decrease of users' training time; and
   - Mitigation of system complexity.

4.3 Summary

This chapter has introduced the reader to the two leading security management vendors: IBM Security and RSA (EMC). IBM InfoSphere Guardium, a data security platform developed by IBM Security, was analyzed first. Following this a description of RSA Archer was also given. The goal of this chapter was to identify the processes offered by both solutions in order to use this knowledge when comparing them with the assurance requirements stated in KSF v3.1.

5 Evaluation with Regard to KSF Assurance Requirements

The purpose of this chapter is to decide whether the capabilities of IBM InfoSphere and RSA Archer satisfy the assurance requirements stated in Swedish Armed Forces' KSF v3.1.

Section 5.1 introduces the concepts related to the assurance requirements. Section 5.2 analyzes *SASS - The system's IT security specification* assurance requirements. Section 5.3 discusses *SALC - System development life cycle* assurance requirements. *SADE - Architecture and design* assurance requirements are discussed in Section 5.4. Section 5.5 analyzes *SAOP - Installation and operation* assurance requirements. Section 5.6 examines assurance requirements for *SARU - Administrative procedures*. Section 5.7 analyzes *SATS - System integration test* assurance requirements. Section 5.8 reviews *SARA - Risk analysis and vulnerability assessment* assurance requirements.

5.1 Assurance requirements

KSF v3.1 divides requirements into two categories: functional and assurance requirements [1] (see Appendix A, Sec. 2.2.1). As previously mentioned, this thesis focuses only on the assurance requirements.

Figure 5-1 shows the requirement identification. The first two letters of each requirement denote either a functional ("SF") or assurance ("SA") requirement. The following two letters denote a class to which a functional or assurance requirement belongs. The three letters following an underline denote a division of this class into different requirements, and the number is used to denote a requirement component.

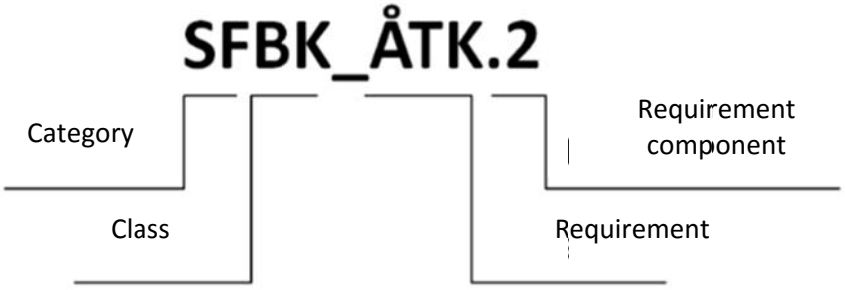

Figure 5-1: Example of requirement identification (Adapted from Figure 5 of [1])

KSF v3.1 [1] (see Appendix A, Sec. 1.7.2) divides assurance requirements into following levels based on the strength of the requirements: High (H), Extended (U), and Ground (G). The level of a specific requirement is determined based on the system exposure level and consequence level. The system exposure is divided into the following levels: E4 (maximum exposure), E3, E2, and E1 (minimum exposure) [1] (see Appendix A, Sec. 2.5.2). On the other hand, the consequence levels of systems are the following: K5 (very serious), K4 (serious), K3 (noticeable), K2 (mild), and K1 (negligible) [1] (see Appendix A, Sec. 2.4).

According to the directions from the Swedish Armed Forces, this thesis will only investigate the exposure level E3 and consequence level K4. Thus, by looking at Table 5-1, it can be concluded that only the assurance requirements of the level **High (H)** will be analyzed. Hence, the requirements that have *high strength* will be denoted by a red coloring (**X**) in the tables in the following sections.

Table 5-1: Determination of assurance requirements level

Consequence level	Exposure level			
	E1	E2	E3	E4
K5	H	H	H	H
K4	U	H	**H**	H
K3	U	U	U	H
K2	G	U	U	U
K1	G	G	G	G

IBM Guardium or RSA Archer may fulfill a certain assurance requirement **completely**, **partially**, or **not at all**.

5.2 SASS - The system's IT security specification

SASS - The system's IT security specification class is used when evaluating whether the IT security specification of a system (ITSS) can serve as a specification for a scheme evaluation [1] (see Appendix C, Sec. 2.1). ITTS should provide a system description, the planned use of the system, and the evaluation that was performed when choosing the system's or system components' exposure and consequence levels [1] (see Appendix A, Sec. 2.7).

This class consists of the following six assurance requirements that will be compared to IBM Guardium and RSA Archer: SASS_INL, SASS_SYS, SASS_KRV, SASS_OMG, and SASS_TOL

5.2.1 SASS_INL – ITSS (IT Security Specification) Introduction

The objective of SASS_INL is the evaluation of the ITSS introduction in order to verify that ITSS is accurately identified. According to KSF v3.1 [1] (see Appendix A, Sec. 2.3.1), an IT system is a system that is evaluated according to KSF. However, that system can also be a "system of systems". Thus, IBM Guardium and RSA Archer are regarded as IT systems. Moreover, IBM Guardium and RSA Archer should create an ITSS with regard to KSF v3.1. However, IBM Guardium and RSA Archer do not provide a specific solution for the Swedish Armed Forces and hence there is no ITSS with regard to KSF v3.1. This represents a limitation that can be solved in the future if the Swedish Armed Forces decide to request a specific solution from IBM or EMC (RSA) that will include an ITSS with regard to KSF. This thesis will investigate whether the solutions from IBM or EMC (RSA) have at least some of the components, which could be included in the ITSS. Table 5-2 describes the required comparison descriptions that are part of SASS_INL, while Table 5-3 describes the degree to which each of IBM InfoSphere and RSA Archer meet these descriptions.

Table 5-2: SASS_INL

SASS_INL	D1	C1	C2	C3	C4	C5	C6	C7	E1
Basic	X	X	X	X	X	X	X	X	X
Extended	X	X	X	X	X	X	X	X	X
High	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**

Table 5-3: SASS_INL Comparison

Requirement Description	IBM Guardium	RSA Archer
SASS_INL.D1 The developer will provide an ITSS Introduction.	Not at all	Not at all
SASS_INL.C1 The ITSS Introduction shall contain an ITSS reference and system overview.	Not at all	Not at all
SASS_INL.C2 The ITSS reference shall uniquely identify the ITSS.	Not at all	Not at all
SASS_INL.C3 IT system reference shall clearly identify the system.	Completely (IBM Guardium provides a reference number for their different versions, e.g., IBM Guardium V9.5 (v9.0 patch 600))	Completely (RSA Archer provides a reference number for their different versions, e.g., RSA Archer Version 5.x)
SASS_INL.C4 IT system reference shall identify the version of the KSF requirements and the requirement level, which ITSS indicates that the system must meet.	Not at all	Not at all
SASS_INL.C5 IT system reference shall identify normative documents, international standards and other security documents as ITSS indicates the system should meet.	Partially (Some standards are specified)	Not at all
SASS_INL.C6 IT system reference shall show which safety requirements in the current requirements collection; the system, and its components shall meet.	Not at all	Not at all
SASS_INL.C7 System overview shall describe the use and security mechanisms in the system at a high level.	Completely	Completely
SASS_INL.E1 The evaluator shall confirm that the information in the dossier meets all requirements for content and presentation	Not at all	Not at all

5.2.2 SASS_SYS – System Description

The objective of SAS_SYS is to evaluate the description of the system in the ITSS [1] (see Appendix C, Sec. 2.1). The system's conditions, interfaces, and security capabilities should be provided. Table 5-4 describes the required comparison descriptions that are part of SASS_SYS, while Table 5-5 describes the degree to which each of IBM InfoSphere and RSA Archer meet these descriptions.

Table 5-4: SASS_SYS

SASS_SYS	D1	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	E1
Basic	X	X	X	X	X	X	X	X	X	X	X	X	X
Extended	X	X	X	X	X	X	X	X	X	X	X	X	X
High	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**

Table 5-5: SASS_SYS Comparison

Requirement Description	IBM Guardium	RSA Archer
SASS_SYS.D1 The system developer shall provide a system description.	Completely	Completely
SASS_SYS.C1 The system description shall describe what information is handled in the system and the consequences that could arise from the loss of this information.	Partially (Critical data is handled but the consequences of the data loss for the Swedish Armed Forces are not described.)	Partially (Critical data is handled but the consequences of the data loss for the Swedish Armed Forces are not described.)
SASS_SYS.C2 The system description should describe the system's exposure.	Partially (IBM InfoSphere Guardium Vulnerability Assessment identifies exposures but Swedish Armed Forces' exposures are not described.)	Partially (RSA Archer identifies exposure by using real-time reports but Swedish Armed Forces' exposures are not described.)
SASS_SYS.C3 Description of system exposure and consequence shall be done with terms that KSF uses.	Not at all	Not at all
SASS_SYS.C4 The system description shall describe the system's intended use, users of the system and information to be stored, processed, transmitted or carried out of the system.	Partially (IBM InfoSphere Guardium does provide a general description but not the specific one for the Swedish Armed Forces.)	Partially (RSA Archer does provide a general description but not the specific one for the Swedish Armed Forces.)

Requirement Description	IBM Guardium	RSA Archer
SASS_SYS.C5 The system description shall describe the system's physical boundaries, and all externally accessible interfaces.	Partially (One of the tasks of IBM InfoSphere Guardium is to identify both the physical and logical boundaries but currently they are not identified for the Swedish Armed Forces.)	Partially (One of the tasks of IBM InfoSphere Guardium is to identify both the physical and logical boundaries but currently they are not identified for the Swedish Armed Forces.)
SASS_SYS.C6 The system description shall describe the purpose and method of use for all externally accessible interfaces.	Not at all	Not at all
SASS_SYS.C7 The system description shall describe the system architecture and design, and to identify the components that the system consists of.	Completely (The architecture and design of IBM InfoSphere Guardium is available.)	Completely (The architecture and design of RSA Archer is available.)
SASS_SYS.C8 The system description shall clearly identify the components that are relevant to security.	Completely (All of the components of IBM InfoSphere Guardium are relevant to security.)	Completely (All of the components of RSA Archer are relevant to security.)
SASS_SYS.C9 The system description shall for all externally accessible interfaces include a description of the individual components that comprise the interface.	Not at all	Not at all
SASS_SYS.C10 The system description shall describe the system's security capabilities and security features provided by the system.	Completely	Completely
SASS_SYS.C11 The description of the system's capabilities must be clear, consistent and agreeable with other parts of ITSS.	Partially	Partially
SASS_SYS.E1 The evaluator shall confirm that the information in the dossier meets all the requirements for content and presentation.	Not at all	Not at all

5.2.3 SASS_KRV – Summary of security requirements

The objective of SASS_KRV is to ensure that the system's security requirements are identified based on the KSF model or some other external requirements [1] (see Appendix C, Sec. 2.1). Table 5-6 describes the required comparison descriptions that are part of SASS_KRV, while Table 5-7 describes the degree to which each of IBM InfoSphere and RSA Archer meet these descriptions.

Table 5-6: SASS_KRV

SASS_KRV	D1	C1	C2	C3	C4	C5	C6	E1
Basic	X	X	X	X	X	X	X	X
Extended	X	X	X	X	X	X	X	X
High	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**

Table 5-7: SASS_KRV Comparison

Requirement Description	IBM Guardium	RSA Archer
SASS_KRV.D1 The system developer shall provide a summary of security requirements.	Not at all	Not at all
SASS_KRV.C1 The summary of security requirements shall identify the requirements that come from the KSF and the requirements for future security requirements.	Not at all	Not at all
SASS_KRV.C2 The summary of KSF requirements shall describe the requirement levels for all requirements, all requirement components, both those that are met by the system and those that must be met by the system environment.	Not at all	Not at all
SASS_KRV.C3 The summary of KSF requirements shall describe the requirement levels of assurance requirements and all applicable requirements components.	Not at all	Not at all
SASS_KRV.C4 Additional security requirements shall identify all security objectives identified in other analyzes carried out (as compulsory business analysis, security analysis, threat, risk and vulnerability, and constitutional analysis).	Not at all	Not at all

Requirement Description	IBM Guardium	RSA Archer
SASS_KRV.C5 The description of the KSF requirements and additional security requirements shall identify the requirements to be met by the system and which should be met by the system environment.	Not at all	Not at all
SASS_KRV.C6 The description of the KSF requirements and future functional requirements shall be clear, consistent and agreeable with other parts of ITSS.	Not at all	Not at all
SASS_KRV.E1 The evaluator shall confirm that the information in the dossier meets all the requirements for content and presentation.	Not at all	Not at all

5.2.4 SASS_OMG – Security requirements for environment

The objective of SASS_OMG is to determine whether the security requirements for the environment of a system are identified and described [1] (see Appendix C, Sec. 2.1). Table 5-8 describes the required comparison descriptions that are part of SASS_OMG, while Table 5-9 describes the degree to which each of IBM InfoSphere and RSA Archer meet these descriptions.

Table 5-8: SASS_OMG

SASS_OMG	D1	C1	C2	C3	C4	C5	E1
Basic	X	X	X	X	X	X	X
Extended	X	X	X	X	X	X	X
High	**X**	**X**	**X**	**X**	**X**	**X**	**X**

Table 5-9: SASS_OMG Comparison

Requirement Description	IBM Guardium	RSA Archer
SASS_OMG.D1 The system developer shall provide security requirements for environment	Completely (e.g.: IBM InfoSphere provides security requirements for Hadoop environment)	Not at all

Requirement Description	IBM Guardium	RSA Archer
SASS_OMG.C1 The security requirements for environment shall identify and describe all the conditions on the system environment necessary for the system to meet their security requirements.	Completely	Not at all
SASS_OMG.C2 The security requirements for the environment shall describe the physical, administrative and organizational measures in the system's environment that fully or partially meet the security requirements for the system's environment.	Partially	Not at all
SASS_OMG.C3 The security requirements for the environment shall identify security requirements and the functional safety requirements for the system derived from the KSF and partly or completely disposed of the system's environment.	Not at all	Not at all
SASS_OMG.C4 The description of the security requirements for the system's environment will clearly show which requirements are met by the system and which are met by the system's environment	Not at all	Not at all
SASS_KRV.C5 The description of the security requirements for the system's environment shall be clear, consistent and consistent with other parts of ITSS.	Not at all	Not at all
SASS_KRV.E1 The evaluator shall confirm that the information in the dossier meets all the requirements for content and presentation.	Not at all	Not at all

5.2.5 SASS_TOL – Interpretation of security

The objective of SASS_TOL is to ensure that system security is interpreted at a system-specific way in order to be precisely translated by the system [1] (see Appendix C, Sec. 2.1). Table 5-10 describes the required comparison descriptions that are part of SASS_TOL, while Table 5-10 describes the degree to which each of IBM InfoSphere and RSA Archer meet these descriptions.

Table 5-10: SASS_TOL

SASS_TOL	D1	C1	C2	C3	C4	E1
Basic	X	X	X	X	X	X
Extended	X	X	X	X	X	X
High	**X**	**X**	**X**	**X**	**X**	**X**

Table 5-11: SASS_TOL Comparison

Requirement Description	IBM Guardium	RSA Archer
SASS_TOL.D1 The system developer shall provide an interpretation of security.	Not at all	Not at all
SASS_TOL.C1 The interpretation of security requirements shall describe the interpretation of all of the security requirements for the system.	Not at all	Not at all
SASS_TOL.C2 The interpretation of security requirements shall specify the functional security requirements so that the interpreted requirements are testable and that a design can be verified against the interpretation of the requirement.	Not at all	Not at all
SASS_TOL.C3 The interpretation of security requirements needs to be as strict or stricter than the original requirements, whether the requirements coming from the KSF or additional security requirements.	Not at all	Not at all
SASS_TOL.C4 The description of the interpretation of the KSF requirements and additional security requirements shall be clear and consistent with other parts of ITSS.	Not at all	Not at all
SASS_TOL.E1 The evaluator shall confirm that the information in the dossier meets all the requirements for content and presentation.	Not at all	Not at all

5.2.6 SASS_UPF – Compliance with security requirements

The objective of SASS_UPF is to ensure that the identified functional security requirements are handled by the system [1] (see Appendix C, Sec. 2.1). Table 5-12 describes the required comparison descriptions that are part of SASS_UPF, while Table 5-13 describes the degree to which each of IBM InfoSphere and RSA Archer meet these descriptions.

Table 5-12: SASS_UPF

SASS_UPF	D1	C1	C2	C3	C4	E1
Basic	X	X	X	X	X	X
Extended	X	X	X	X	X	X
High	**X**	**X**	**X**	**X**	**X**	**X**

Table 5-13: SASS_UPF Comparison

Requirement Description	IBM Guardium	RSA Archer
SASS_UPF.D1 The system developer shall provide compliance with security requirements.	Not at all	Not at all
SASS_UPF.C1 Compliance with security requirements should show how all the security requirements in the chapter *Interpretation of the security requirements* have been met by the system security features.	Not at all	Not at all
SASS_UPF.C2 Compliance with security requirements should demonstrate that all requirements are met entirely by the system.	Not at all	Not at all
SASS_UPF.C3 Compliance with safety requirements shall for each requirement show that all requirements have been met by the system.	Not at all	Not at all
SASS_UPF.C4 The description of the fulfillment of the security requirements shall be clear, consistent and agreeable with other parts of ITSS.	Not at all	Not at all
SASS_UPF.E1 The evaluator shall confirm that the information in the dossier meets all the requirements for content and presentation.	Not at all	Not at all

5.3 SALC - System development life cycle

SALC – System development life cycle [1] (see Appendix C, Sec. 2.2) is used in order to gain confidence in the system management, starting from the system design, system development, etc. The first requirement of having confidence in the system is to have confidence in the system origin and system components. Moreover, it is important to ensure that the changes in the system and its components are performed under controlled conditions.

This class consists of the following five assurance requirements that will be compared to IBM Guardium and RSA Archer: SALC_UTV, SALC_KFG, SALC_LEV, SALC_LCM, and SALC_BRK

5.3.1 SALC_UTV – Development security

The objective of SALC_UTV is to analyze the origin of the system and its components, security of the system development environment, and access to critical data that has an impact on the overall confidence in the system [1] (see Appendix C, Sec. 2.2). Table 5-14 describes the required comparison descriptions that are part of SALC_UTV, while Table 5-15 describes the degree to which each of IBM InfoSphere and RSA Archer meet these descriptions.

Table 5-14: SALC_UTV

SALC_UTV	D1	D2	D3	D4	C1	C2	C3	C4	C5	C6	E1	E2
Basic												
Extended	X	X	X	X	X	X	X	X			X	X
High	**X**	**X**	**X**	**X**	**X**	**X**			**X**	**X**	**X**	**X**

Table 5-15: SALC_UTV Comparison

Requirement Description	IBM Guardium	RSA Archer
SALC_UTV.D1 The system developer shall provide system development documentation.	Partially	Partially
SALC_UTV.D2 System developer shall apply system development documentation.	Not at all	Not at all
SALC_UTV.D3 The system developer shall provide integration documentation.	Completely (IBM InfoSphere Guardium describes its integration capabilities.)	Completely (RSA provides RSA Archer Integration Guide)
SALC_UTV.D4 The system developer shall provide acceptance criteria for components that will be included in the system.	Not at all	Not at all

Requirement Description	IBM Guardium	RSA Archer
SALC_UTV.C1 System documentation shall describe the physical, logical, administrative, personnel and other security measures necessary to ensure the privacy and accuracy of the design and implementation of the system in the development environment.	Partially	Partially
SALC_UTV.C2 System development documentation shall show that the security measures provide an accurate protection of the development environment.	Completely	Completely
SALC_UTV.C5 The acceptance criteria shall describe sufficient criteria for acceptance and verification of safety-related components included in the system.	Not at all	Not at all
SALC_UTV.C6 Integration documentation shall identify the origins of all the components and document that the origin was identified and how the acceptance inspection took place.	Not at all	Not at all
SALC_UTV.E1 The evaluator shall confirm that the information in the dossier meets all the requirements for content and presentation.	Not at all	Not at all
SALC_UTV.E2 The evaluator shall verify that the system development documentation applies security measures.	Not at all	Not at all

5.3.2 SALC_KFG – Configuration management

The objective of SALC_KFG is to analyze the configuration management regarding the system components [1] (see Appendix C, Sec. 2.2). Table 5-16 describes the required comparison descriptions that are part of SALC_KFG, while Table 5-17 describes the degree to which each of IBM InfoSphere and RSA Archer meet these descriptions.

Table 5-16: SALC_KFG

SALC_KFG	D1	D2	D3	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	E1	E2
Basic															
Extended	X	X	X	X	X	X	X	X	X	X	X	X		X	X
High	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**

Table 5-17: SALC_KFG Comparison

Requirement Description	IBM Guardium	RSA Archer
SALC_KFG.D1 The system developer shall provide the system and a unique system reference.	Completely (E.g.: Reference number of IBM InfoSphere Guardium is 1609224 for Linux OS)	Not at all
SALC_KFG.D2 The system developer shall use a configuration management system.	Not at all	Completely (RSA Archer integrates configuration management system.)
SALC_KFG.D3 The system developer shall provide documentation describing the configuration management system.	Not at all	Partially
SALC_KFG.C1 The IT system and its components must be marked with a unique reference.	Completely	Not at all
SALC_KFG.C2 The documentation describing the configuration management will demonstrate methods for unique identification of configuration-driven IT components.	Not at all	Not at all
SALC_KFG.C3 The documentation describing the configuration management will demonstrate how configuration management used in system development and system developer's management of the system.	Not at all	Not at all
SALC_KFG.C4 All configuration items included in the system shall be under configuration management.	Not at all	Not at all
SALC_KFG.C5 The documentation describing the configuration management shall describe the acceptance procedures for new and updated configuration	Not at all	Not at all

Requirement Description	IBM Guardium	RSA Archer
items.		
SALC_KFG.C6 The documentation describing the configuration management shall demonstrate that the acceptance procedures used provide adequate change management for all configuration items.	Not at all	Not at all
SALC_KFG.C7 Documentation must prove that the system for configuration management is conducted in accordance with the documentation of configuration management.	Not at all	Not at all
SALC_KFG.C8 Documentation must demonstrate that all components and its parts, all assurance documents, reports of potential safety and other documentation that describes the provider's management of the system are under the control of configuration management.	Not at all	Not at all
SALC_KFG.C9 Configuration management system shall provide security measures for change management that ensure that all changes are implemented in a controlled manner and by qualified personnel.	Not at all	Partially
SALC_KFG.C10 Configuration management system shall include the technical features for traceability that ensures that all changes can clearly be traced to the individual who conducted them.	Not at all	Partially
SALC_KFG.E1 The evaluator shall confirm that the information in the dossier meets all the requirements for content and presentation.	Not at all	Not at all
SALC_KFG.E2 The evaluator shall verify that the configuration management system applies security measures.	Not at all	Not at all

5.3.3 SALC_LEV – System delivery

The objective of SALC_LEV is to ensure that the system delivery procedures are performed in a secure manner [1] (see Appendix C, Sec. 2.2). Hence, the goal is to prevent or detect any loss that could harm the systems' security. Table 5-18 describes the required comparison descriptions that are part of SALC_LEV, while Table 5-19 describes the degree to which each of IBM InfoSphere and RSA Archer meet these descriptions.

Table 5-18: SALC_LEV

SALC_LEV	D1	D2	C1	C2	C3	E1
Basic	X	X	X	X		X
Extended	X	X	X	X	X	X
High	**X**	**X**	**X**	**X**	**X**	**X**

Table 5-19: SALC_LEV Comparison

Requirement Description	IBM Guardium	RSA Archer
SALC_LEV.D1 The system developer shall provide documentation describing the procedures and mechanisms for the IT system and component deliveries.	Completely	Not at all
SALC_LEV.D2 The system developer shall use the delivery procedures.	Completely	Not at all
SALC_LEV.C1 Delivery documentation shall describe all procedures that are necessary to maintain the security of the system during its delivery to the operating and management organization.	Not at all	Not at all
SALC_LEV.C2 Delivery documentation shall describe how the system's accuracy is protected during delivery.	Not at all	Not at all
SALC_LEV.C3 Delivery documentation shall describe how the system accuracy can be verified by the recipient upon delivery and at any time after delivery.	Partially (Verification is done based on the reports but there is no delivery documentation describing this.)	Not at all
SALC_LEV.E1 The evaluator shall confirm that the information in the dossier meets all the requirements for content and presentation.	Not at all	Not at all

5.3.4 SALC_LCM – Lifecycle model

The objective of SALC_LCM is to evaluate the lifecycle model for the system development [1] (see Appendix C, Sec. 2.2). Elementary life cycle model components are test and acceptance procedures that are used when designing, developing, and delivering the system. Table 5-20 describes the required comparison descriptions that are part of SALC_LCM, while Table 5-21 describes the degree to which each of IBM InfoSphere and RSA Archer meet these descriptions.

Table 5-20: SALC_LCM

SALC_LCM	D1	D2	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	E1	E2
Basic														
Extended	X	X	X	X	X	X	X	X	X	X			X	X
High	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**

Table 5-21: SALC_LCM Comparison

Requirement Description	IBM Guardium	RSA Archer
SALC_LCM.D1 The system developer shall establish a lifecycle model to be used in the development of the system and the system developer's management of the system.	Completely	Completely
SALC_LCM.D2 The system developer shall provide documentation that describes the lifecycle model.	Completely	Completely
SALC_LCM.C1 The lifecycle model shall include system development and system developer's management of the system.	Completely	Completely
SALC_LCM.C2 The lifecycle model shall provide control over system development and system developer's management of the system.	Not at all	Not at all
SALC_LCM.C3 The lifecycle model shall describe the need to assess the security impact of changes in the system during the system's life cycle.	Completely	Completely

Requirement Description	IBM Guardium	RSA Archer
SALC_LCM.C4 The lifecycle model shall describe the need to maintain the security of the system during its life cycle and systems developer's management of the system.	Completely	Completely
SALC_LCM.C5 The lifecycle model will describe the parts of the design, operation and management documentation necessary to maintain security during the system's life cycle.	Completely	Completely
SALC_LCM.C6 The lifecycle model shall describe procedures for verification of components suitability for use in the system	Not at all	Not at all
SALC_LCM.C7 The lifecycle model shall describe the acceptance and release procedures for system design and the components.	Not at all	Not at all
SALC_LCM.C8 The lifecycle model shall describe how quality is integrated into the system lifecycle.	Partially	Partially
SALC_LCM.C9 The life-cycle model shall describe how the process for quality assurance meets similar requirements of ISO 9001	Not at all	Not at all
SALC_LCM.C10 The procedures for verification of components suitability for use in the system shall include the judgment of each component's security impact on the system.	Not at all	Not at all
SALC_LCM.E1 The evaluator shall verify that the information in the dossier meets all requirements for content and presentation.	Not at all	Not at all
SALC_LCM.E2 The evaluator shall verify that the life cycle model is applied.	Not at all	Not at all

5.3.5 SALC_BRK – Fault correction

The objective of SALC_BRK is to analyze the fault correction procedures in the system [1] (see Appendix C, Sec. 2.2). Table 5-22 describes the required comparison descriptions that are part of SALC_BRK, while Table 5-23 describes the degree to which each of IBM InfoSphere and RSA Archer meet these descriptions.

Table 5-22: Fault correction

SALC_BRK	D1	D2	D3	D4	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	E1
Basic	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Extended	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
High	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**

Table 5-23: SALC_BRK Comparison

Requirement Description	IBM Guardium	RSA Archer
SALC_BRK.D1 The system developer shall provide documented procedures for the handling of security-related defects in the system.	Completely	Completely
SALC_BRK.D2 The system developer should have the necessary agreements and processes to get information about the security-relevant flaws in the system and components	Completely	Completely
SALC_BRK.D3 The system developer shall provide operational and administrative documentation of security-related defects in the system.	Completely	Completely
SALC_BRK.D4 System developer shall establish a process for reporting security-related defects in the system.	Completely	Completely
SALC_BRK.C1 Operation and management documentation shall describe how the operational and administrative organization can report suspected security-related defects in the system.	Completely	Completely

Requirement Description	IBM Guardium	RSA Archer
SALC_BRK.C2 Operation and management documentation shall identify specific contact for all reports and inquiries about security-relevant flaws in the system.	Completely	Completely
SALC_BRK.C3 Documented procedures for the management of security-related defects in the system shall describe methods for the safe delivery of information about the faults, fault correction, and security updates to the operating and management organization.	Completely	Completely
SALC_BRK.C4 Documented procedures for the management of security-related defects in the system shall ensure that corrective actions are identified for all known security-related deficiencies.	Completely	Completely
SALC_BRK.C5 The documentation describing the handling of security-related deficiencies shall describe how the information about the shortcomings and instructions on remedies provided operating and management organization.	Completely	Completely
SALC_BRK.C6 Documented procedures for the management of security-related defects in the system shall ensure that all known security-related deficiencies are remedied and that security updates are issued to the operating and management organization.	Completely	Completely
SALC_BRK.C7 Documented procedures for the management of security-related defects in the system shall ensure that security updates do not introduce any new security flaws or deficiencies.	Completely	Completely

Requirement Description	IBM Guardium	RSA Archer
SALC_BRK.C8 The documentation describing the handling of security-related deficiencies shall describe the procedures used to track all reported security flaws in the system in every release.	Completely	Completely
SALC_BRK.C9 The documentation describing the handling of security-related deficiencies shall describe how the operational and administrative documentation categorizes the nature and effect of each security-relevant deficiency and the status of corrective actions.	Completely	Completely
SALC_BRK.C10 Documented procedures for the management of security-related deficiencies in the system shall ensure that all components are integrated in the process of handling security-relevant deficiencies in the system.	Completely	Completely
SALC_BRK.E1 The evaluator shall verify that the information in the dossier meets all requirements for content and presentation.	Not at all	Not at all

5.4 SADE - Architecture and design

SADE – Architecture and design [1] (see Appendix C, Sec. 2.3) is used in order to gain confidence in the architecture and design of a system. Thus, the architecture and design must be properly described and non-contradictory.

This class consists of the following four assurance requirements that will be compared to IBM Guardium and RSA Archer: SADE_GRÄ, SADE_ARK, SADE_DFA, and SADE_DES.

5.4.1 SADE_GRÄ – Interface description

The objective of SADE_GRÄ is to evaluate whether the system's external interfaces are identified, and the security-related issues are determined [1] (see Appendix C, Sec. 2.3). Table 5-24 describes the required comparison descriptions that are part of SADE_GRÄ, while Table 5-25 describes the degree to which each of IBM InfoSphere and RSA Archer meet these descriptions.

Table 5-24: SADE_GRÄ

SADE_GRÄ	D1	C1	C2	C3	C4	E1
Basic						
Extended	X	X	X	X	X	X
High	**X**	**X**	**X**	**X**	**X**	**X**

Table 5-25: SADE_GRÄ Comparison

Requirement Description	IBM Guardium	RSA Archer
SADE_GRÄ.D1 The system developer shall provide a description of system interfaces.	Completely	Completely
SADE_GRÄ.C1 The description of the system's interfaces shall include an analysis of which externally accessible interfaces are security-relevant and which are not.	Completely	Completely
SADE_GRÄ.C2 The description of the system's interfaces shall contain a description of the security relevant actions associated with each security-relevant interface.	Completely	Completely
SADE_GRÄ.C3 The description of the system's interfaces shall include a summary of the security features that are associated with the respective interface.	Partially	Partially
SADE_GRÄ.C4 The description of the system's interfaces shall include complete description of the interaction system all externally accessible interfaces allow.	Not at all	Not at all
SADE_GRÄ.E1 The evaluator shall verify that the information in the dossier meets all requirements for content and presentation.	Not at all	Not at all

5.4.2 SADE_ARK – Security architecture

The objective of SADE_ARK is to evaluate whether the security architecture of a system is described. Moreover, security-relevant system components and dependencies between them are

analyzed [1] (see Appendix C, Sec. 2.3). Table 5-26 describes the required comparison descriptions that are part of SADE_ARK, while Table 5-27 describes the degree to which each of IBM InfoSphere and RSA Archer meet these descriptions.

Table 5-26: SADE_ARK

SADE_ARK	D1	D2	C1	C2	C3	E1	E2
Basic							
Extended	X	X	X	X	X	X	X
High	**X**	**X**	**X**	**X**	**X**	**X**	**X**

Table 5-27: SADE_ARK Comparison

Requirement Description	IBM Guardium	RSA Archer
SADE_ARK.D1 The system developer shall provide a description of the system's security architecture.	Completely	Completely
SADE_ARK.D2 System developer shall design and implement the system so that the security features cannot be bypassed.	Completely	Completely
SADE_ARK.C1 The description of the security architecture shall demonstrate how the components and their interactions result in system security functionality.	Completely	Completely
SADE_ARK.C2 The security architecture shall for every security-relevant component identify other components that it depends on and how it depends on the other components.	Completely	Completely
SADE_ARK.C3 The description of the security architecture shall demonstrate that the system architecture prevents security functionality to be bypassed.	Completely	Completely
SADE_ARK.E1 The evaluator shall verify that the information in the dossier meets all requirements for content and presentation.	Not at all	Not at all
SADE_ARK.E2 The evaluator shall analyze the documentation and verify that it is not possible to bypass the system's security features.	Not at all	Not at all

5.4.3 SADE_DFA - Data Flow Analysis

The objective of SADE_DFA is the identification of system's components that are responsible for storage and processing of critical data in the system [1] (see Appendix C, Sec. 2.3). Table 5-28 describes the required comparison descriptions that are part of SADE_DFA, while Table 5-29 describes the degree to which each of IBM InfoSphere and RSA Archer meet these descriptions.

Table 5-28: SADE_DFA

SADE_DFA	D1	C1	C2	C3	C4	C5	E1
Basic							
Extended	X	X	X	X	X		X
High	**X**	**X**	**X**	**X**	**X**	**X**	**X**

Table 5-29: SADE_DFA Comparison

Requirement Description	IBM Guardium	RSA Archer
SADE_DFA.D1 The system developer shall provide a data flow analysis of critical data in the system.	Completely	Completely
SADE_DFA.C1 Data flow analysis shall identify all critical data stored and processed by the system.	Completely	Completely
SADE_DFA.C2 Data flow analysis shall include a consequence level analysis of the critical data stored or processed by the system components.	Completely	Completely
SADE_DFA.C3 Data flow analysis shall document the components that store or process the critical data as well as the components that do not process or store the critical data.	Completely	Completely
SADE_DFA.C4 Data flow analysis shall document how critical data is transferred between components in the system.	Completely	Completely
SADE_DFA.C5 Data flow analysis shall consider all the critical Data flow analysis must consider all the data critical and therefore fully describe the all system data flows and therefore fully describe the system data flows.	Completely	Completely
SADE_DFA.E1 The evaluator shall verify that the information in the dossier meets all requirements for content and presentation.	Not at all	Not at all

5.4.4 SADE_DES – Design documentation

The objective of SADE_DES is to evaluate the impact of components on the system security, and the integration of components into the system [1] (see Appendix C, Sec. 2.3). Table 5-30 describes the required comparison descriptions that are part of SADE_DES, while Table 5-31 describes the degree to which each of IBM InfoSphere and RSA Archer meet these descriptions.

Table 5-30: SADE_DES

SADE_DES	D1	C1	C2	C3	C4	C5	C6	E1
Basic								
Extended	X	X	X	X	X	X		X
High	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**

Table 5-31: SADE_DES Comparison

Requirement Description	IBM Guardium	RSA Archer
SADE_DES.D1 The system developer shall provide design documentation for the system.	Completely	Completely
SADE_DES.C1 The design shall describe the structure of the system in terms of its components.	Completely	Completely
SADE_DES.C2 The design shall identify components that contribute to the security functionality of the system.	Completely	Completely
SADE_DES.C3 The design shall describe each component's behavior sufficiently in order to determine what components are security-relevant.	Completely	Completely
SADE_DES.C4 The design shall include a description of the interaction between the security-relevant components and between security-relevant and non-security-relevant components.	Partially	Partially
SADE_DES.C5 Design documentation shall demonstrate that any externally accessible interface identified in the interface description is associated with at least one security-relevant component.	Not at all	Not at all

Requirement Description	IBM Guardium	RSA Archer
SADE_DES.C6 Design documentation shall demonstrate how the system components and their configuration give the system its intended IT security capabilities.	Completely	Completely
SADE_DES.E1 The evaluator shall verify that the information in the dossier meets all requirements for content and presentation.	Not at all	Not at all

5.5 SAOP - Installation and operation

SAOP – Installation and operation [1] (see Appendix C, Sec. 2.4) is used in order to confirm that the installation, implementation, management, and maintenance of a system can be performed securely.

This class consists of the following three assurance requirements that will be compared to IBM Guardium and RSA Archer: SAOP_INS, SAOP_DOK, and SAOP_BRK.

5.5.1 SAOP_INS – Installation and preparation

The objective of SAOP_INS is to confirm that the acceptation and installation of a system in its operating environment will be performed securely and as planned [1] (see Appendix C, Sec. 2.4). Table 5-32 describes the required comparison descriptions that are part of SAOP_INS, while Table 5-33 describes the degree to which each of IBM InfoSphere and RSA Archer meet these descriptions.

Table 5-32: SAOP_INS

SAOP_INS	D1	C1	C2	C3	C4	E1	E2
Basic	X	X	X	X		X	
Extended	X	X	X	X	X	X	X
High	**X**	**X**	**X**	**X**	**X**	**X**	**X**

Table 5-33: SAOP_INS Comparison

Requirement Description	IBM Guardium	RSA Archer
SAOP_INS.D1 The system developer shall provide the system with documentation describing the preparatory actions.	Completely (IBM InfoSphere Guardium Installation Guide & Deployment Guide for InfoSphere Guardium)	Completely (RSA Archer Installation Guide)

Requirement Description	IBM Guardium	RSA Archer
SAOP_INS.C1 The preparatory actions shall describe all the steps necessary to safely accept the delivered system in accordance with the developer's system delivery procedure (SALC_LEV).	Completely	Completely
SAOP_INS.C2 The preparatory actions shall describe all the necessary steps for the safe installation of the system.	Completely	Completely
SAOP_INS.C3 The preparatory actions shall include the steps to ensure that the operating environment meets the requirements of the operating environment as documented in ITSS (SASS_OMG).	Not at all	Not at all
SAOP_INS.C4 The preparatory actions shall include steps for verification of the correct installation.	Completely	Completely
SAOP_INS.E1 The evaluator shall verify that the information in the dossier meets all requirements for content and presentation.	Not at all	Not at all
SAOP_INS.E2 The evaluator shall implement measures to verify that the system can be received and installed safely by following the description of them.	Not at all	Not at all

5.5.2 SAOP_DOK – Operating and administration documentation

The objective of SAOP_DOK is to analyze the operating and administration documentation of a system [1] (see Appendix C, Sec. 2.4). Table 5-34 describes the required comparison descriptions that are part of SAOP_DOK, while Table 5-35 describes the degree to which each of IBM InfoSphere and RSA Archer meet these descriptions.

Table 5-34: SAOP_DOK

SAOP_DOK	D1	C1	C2	C3	C4	C5	C6	C7	C8	E1
Basic	X	X	X	X	X	X	X	X	X	X
Extended	X	X	X	X	X	X	X	X	X	X
High	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**

Table 5-35: SAOP_DOK Comparison

Requirement Description	IBM Guardium	RSA Archer
SAOP_DOK.D1 The system developer shall provide operating and administration documentation.	Completely (IBM Guardium Administrator Responsibilities Guide)	Completely (RSA Archer Administrator Guide)
SAOP_DOK.C1 Operating and administration documentation shall for each user role describe the user interface and security features available to the user.	Completely	Completely
SAOP_DOK.C2 Operating and administration documentation shall for each user role describe how the available user interface provided by the system shall be used securely. This includes all the security parameters that the user can change and what values they can consider secure.	Completely	Completely
SAOP_DOK.C3 Operating and administration documentation shall for each user role clearly describe each type of security-relevant activity linked to the available user actions that must perform comprehensive operation and maintenance of security functions.	Partially	Partially
SAOP_DOK.C4 Operating and administration documentation shall identify all possible modes of operation in the system, including the operation after the fault occurred if the system ends up in an uncertain situation, its consequences and implications for the continued secure operation of the system.	Completely	Completely
SAOP_DOK.C5 Operating and administration documentation shall describe all security requirements that the system and its components impose on the environment and other components that are managed by the operating environment of each user role.	Completely	Partially

Requirement Description	IBM Guardium	RSA Archer
SAOP_DOK.C6 Operating and administration documentation shall for each respective user role document all allowed system configurations critical dependencies between the various component configurations.	Not at all	Not at all
SAOP_DOK.C7 Operating and administration documentation shall describe procedures for reporting security-related events, such as loss of equipment or cleared security attributes.	Completely	Completely
SAOP_DOK.C8 Operating and administration documentation shall be clear and appropriate for the intended users.	Completely	Completely
SAOP_DOK.E1 The evaluator shall verify that the information in the dossier meets all requirements for content and presentation.	Not at all	Not at all

5.5.3 SAOP_BRK – Fault correction

The objective of SAOP_BRK is to confirm that security-related deficiencies in a system are handled by the operating and administration organization [1] (see Appendix C, Sec. 2.4). Table 5-36 describes the required comparison descriptions that are part of SAOP_BRK, while Table 5-37describes the degree to which each of IBM InfoSphere and RSA Archer meet these descriptions.

Table 5-36: SAOP_BRK Comparison

SAOP_BRK	D1	D2	C1	C2	C3	C4	C5	C6	C7	C8	E1
Basic	X	X	X	X	X	X	X	X	X	X	X
Extended	X	X	X	X	X	X	X	X	X	X	X
High	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**

Table 5-37: SAOP_BRK Comparison

Requirement Description	IBM Guardium	RSA Archer
SAOP_BRK.D1 The system developer shall provide instructions that enable operating and administration organization to carry out monitoring of the faults and fault correction.	Completely	Completely
SAOP_BRK.D2 The system developer shall make the necessary contacts to operating and administration organization for fault correction information for the system components to be monitored.	Not at all	Not at all
SAOP_BRK.C1 The instructions shall include processes for monitoring of information sources regarding security-related defects in the system and its components.	Completely	Completely
SAOP_BRK.C2 The instructions shall include processes so that security-related deficiencies are followed up and corrected.	Completely	Completely
SAOP_BRK.C3 The instructions shall describe how the monitoring of security-related deficiencies shall be documented and demonstrate that the documentation should contain sources, analysis, conclusion and recommended actions.	Completely	Completely
SAOP_BRK.C4 The instructions shall include processes for the integration of security updates in the system, including the uninstallation.	Not at all	Not at all
SAOP_BRK.C5 The instructions shall include methods for secure receipt of fault information and a fault correction of the system and its components.	Completely	Completely
SAOP_BRK.C6 The instructions shall include procedures for the verification of the existence and origin of security updates before they enter the system.	Not at all	Not at all

Requirement Description	IBM Guardium	RSA Archer
SAOP_BRK.C7 The life-cycle model shall include procedures to determine whether a fixed fault in a component is security-relevant and shall be introduced and how it will be accepted.	Not at all	Not at all
SAOP_BRK.C8 The instructions shall include procedures for testing security updates to ensure that the security functionality is still intact after the introduction.	Not at all	Not at all
SAOP_BRK.E1 The evaluator shall verify that the information in the dossier meets all requirements for content and presentation.	Not at all	Not at all

5.6 SARU - Administrative procedures

SARU – Administrative procedures [1] (see Appendix C, Sec. 2.5) is used when confirming that the system documentation contains all the administrative procedures that are necessary for the administration of system's security functions.

This class consists of the following six assurance requirements that will be compared to IBM Guardium and RSA Archer: SARU_ ÅTK, SARU_ATT, SARU_INT, SARU_UPD, SARU_KFG, and SARU_UTB.

5.6.1 SARU_ÅTK – Access rights

The objective of SARU_ÅTK is to confirm that the user rights are being handled by the system's administrative procedures [1] (see Appendix C, Sec. 2.5). Table 5-38 describes the required comparison descriptions that are part of SARU_ÅTK, while Table 5-39 describes the degree to which each of IBM InfoSphere and RSA Archer meet these descriptions.

Table 5-38: SARU_ÅTK

SARU_ÅTK	D1	C1	C2	C3	C4	C5	C6	C7	C8	C9	E1
Basic	X	X	X	X	X	X					X
Extended	X	X	X	X	X	X	X	X		X	X
High	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**

Table 5-39: SARU_ÅTK Comparison

Requirement Description	IBM Guardium	RSA Archer
SARU_ÅTK.D1 The system developer shall provide documented administrative procedures for the allocation and revocation of access rights.	Completely (IBM Guardium Access Management Help Book)	Completely (RSA Archer GRC Platform)
SARU_ÅTK.C1 The procedures shall describe how access rights are assigned and revoked.	Completely	Completely
SARU_ÅTK.C2 The procedures shall show access rights as a general rule assigned to roles (or groups) and describe the cases where specific access rights may need to be assigned directly to the subject.	Completely	Completely
SARU_ÅTK.C3 The procedures shall show that a user or subject is assigned to the roles (and groups) that they are authorized to, and are necessary for their service.	Completely	Completely
SARU_ÅTK.C4 The procedures shall describe how the follow-up of the assignment is made to ensure that the system users and subjects have been properly assigned to roles and access rights.	Completely	Completely
SARU_ÅTK.C5 The procedures shall describe that only the authorized personnel are assigned access rights to administrative functions for safety functions, their configuration and management of data.	Completely	Completely

Requirement Description	IBM Guardium	RSA Archer
SARU_ÅTK.C6 The procedures shall describe a person may not be assigned access rights to more than one of the following functions or roles: • Administration of access control; • Administration of security log; and • Other operating administration.	Not at all	Not at all
SARU_ÅTK.C7 The procedures shall describe that a person who is assigned access rights to functions for administration of intrusion protection is not at the same time assigned access rights to initiate information transfers controlled by the intrusion protection.	Not at all	Not at all
SARU_ÅTK.C8 The procedures shall describe that a person may not be assigned access rights to more than one of the following functions or roles: • Administration of identities and security attributes for authentication; and • Assigning roles and access rights to users or subjects.	Not at all	Not at all
SARU_ÅTK.C9 The procedures shall describe that only the person responsible for the administration of the security log can be assigned access rights to system security logs.	Not at all	Not at all
SARU_ÅTK.E1 The evaluator shall verify that the information in the dossier meets all requirements for content and presentation.	Not at all	Not at all

5.6.2 SARU_ATT - Security attribute for authentication

The objective of SARU_ATT is to confirm that the quality of security attributes that are used for the authentication is checked by the administrative procedures [1] (see Appendix C, Sec. 2.5). Table 5-40 describes the required comparison descriptions that are part of SARU_ATT, while Table 5-41 describes the degree to which each of IBM InfoSphere and RSA Archer meet these descriptions.

Table 5-40: SARU_ATT

SARU_ATT	D1	C1	C2	C3	C4	C5	C6	C7	E1
Basic	X	X	X	X	X	X	X	X	X
Extended	X	X	X	X	X	X	X	X	X
High	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**

Table 5-41: SARU_ATT Comparison

Requirement Description	IBM Guardium	RSA Archer
SARU_ATT.D1 The system developer shall provide documented administrative procedures to control the quality of security attributes used for authentication.	Completely (IBM Guardium Authentication Configuration panel)	Not at all
SARU_ATT.C1 The procedures shall describe a minimum acceptable level of quality for passwords chosen by users.	Completely (Password validation)	Not at all
SARU_ATT.C2 The procedures shall describe that all the assigned passwords are randomly generated and how this happens.	Completely (An 8-digit random number is generated)	Not at all
SARU_ATT.C3 The procedures shall show that randomly generated passwords always consist of at least 12 characters.	Not at all	Not at all
SARU_ATT.C4 The procedures shall demonstrate that passwords are changed during commissioning of the system and operating with a fixed interval.	Partially (Number of days after which a password is expired can be set.)	Not at all
SARU_ATT.C5 The procedures shall describe the regular updating of certificate revocation lists.	Not at all	Not at all

Requirement Description	IBM Guardium	RSA Archer
SARU_ATT.C6 The procedures shall demonstrate that each user identity in the system can be bound to a specific person.	Completely	Not at all
SARU_ATT.C7 The procedures shall describe how the monitoring of system subjects should be made to ensure that only authorized users subject has valid security attributes for authentication.	Completely	Not at all
SARU_ATT.E1 The evaluator shall verify that the information in the dossier meets all requirements for content and presentation.	Not at all	Not at all

5.6.3 SARU_INT - Detect and track intrusion and abuse

The objective of SARU_INT is to verify that the information needed for detection and tracking of intrusion and abuse is handled by the administrative procedures [1] (see Appendix C, Sec. 2.5). Table 5-42 describes the required comparison descriptions that are part of SARU_INT, while Table 5-43 describes the degree to which each of IBM InfoSphere and RSA Archer meet these descriptions.

Table 5-42: SARU_INT

SARU_INT	D1	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	E1
Basic	X	X	X	X	X	X	X	X	X	X	X	X
Extended	X	X	X	X	X	X	X	X	X	X	X	X
High	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**

Table 5-43: SARU_INT Comparison

Requirement Description	IBM Guardium	RSA Archer
SARU_INT.D1 The system developer shall provide documented administrative procedures to detect and track intrusion and abuse in the system.	Completely	Completely
SARU_INT.C1 The procedures shall describe how long the security logs shall be saved and show that they comply with at least the duration that the current regulations dictate.	Not at all	Not at all

Requirement Description	IBM Guardium	RSA Archer
SARU_INT.C2 The procedures shall describe how and with what regularity the utility based analysis of the events recorded in the security log should be.	Not at all	Not at all
SARU_INT.C3 The procedures shall describe how analysis of operational-related error events in the system should be and how it should be documented.	Partially	Partially
SARU_INT.C4 The procedures shall describe how the analysis results are classified and show how the classification decision and the decision on action are documented.	Not at all	Not at all
SARU_INT.C5 The procedures shall describe that the analysis and classification of analyzes results are performed only by a trained operator.	Completely	Completely
SARU_INT.C6 The procedures shall describe how the reports on security events, such as loss of equipment or cleared security attributes should be handled and what measures should be taken.	Completely	Completely
SARU_INT.C7 The procedures shall describe how all identified incidents should be investigated and reported.	Completely	Completely
SARU_ATT.C8 The procedures shall describe how security backup of security log should be done regularly to other storage.	Not at all	Not at all
SARU_INT.C9 The procedures shall describe how security backup of security log should be stored and show that it must be kept physically separate from the security log.	Not at all	Not at all

Requirement Description	IBM Guardium	RSA Archer
SARU_INT.C10 The procedures should describe that the analysis results continue to be managed in accordance with its established IT security plan.	Completely	Completely
SARU_INT.E1 The evaluator shall verify that the information in the dossier meets all requirements for content and presentation.	Not at all	Not at all

5.6.4 SARU_UPD – Security updates

The objective of SARU_UPD is to confirm that the regular system security updates are managed and described by the procedures [1] (see Appendix C, Sec. 2.5). Table 5-44 describes the required comparison descriptions that are part of SARU_UPD, while Table 5-45 describes the degree to which each of IBM InfoSphere and RSA Archer meet these descriptions.

Table 5-44: SARU_UPD

SARU_UPD	D1	C1	C2	C3	C4	C5	C6	C7	C8	E1
Basic	X	X	X	X	X	X	X	X	X	X
Extended	X	X	X	X	X	X	X	X	X	X
High	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**

Table 5-45: SARU_UPD Comparison

Requirement Description	IBM Guardium	RSA Archer
SARU_UPD.D1 The system developer shall provide documented administrative procedures to perform regular backups of system.	Completely (Monthly backups are performed.)	Completely (Automatic backups that can be manually enabled or disabled.)
SARU_UPD.C1 The procedures shall contain detailed instructions for managing security updates for the entire software in the system.	Completely	Completely
SARU_UPD.C2 The procedures shall describe the processes for the secure update of the security features that are dependent on external supply of safety mechanisms or governing data.	Not at all	Not at all

Requirement Description	IBM Guardium	RSA Archer
SARU_UPD.C3 The procedures shall describe that the updates of the security functions control mechanisms and their governing data should be verified for accuracy and origin before they enter the system.	Completely	Completely
SARU_UPD.C4 The procedures shall demonstrate that all security-related defects in the system must be corrected within a documented interval of time from the moment of noticing them.	Not at all	Not at all
SARU_UPD.C5 The procedures shall describe that the security updates to any components of the system should be introduced as soon as possible after they have been made available.	Not at all	Not at all
SARU_UPD.C6 The procedures shall describe that the correctness and origin of security updates have to be verified before they are introduced into the system.	Not at all	Not at all
SARU_UPD.C7 The procedures shall describe how compliance with the procedures for fault management and security updating are documented so that checks can be easily implemented.	Not at all	Not at all
SARU_UPD.C8 The procedures shall describe how the risk minimization measures should be taken immediately after a security-related system weakness is identified.	Completely	Completely
SARU_UPD.E1 The evaluator shall verify that the information in the dossier meets all requirements for content and presentation.	Not at all	Not at all

5.6.5 SARU_KFG – Configuration control

The objective of SARU_KFG is to confirm that the configuration management system can be implemented by the operating personnel [1] (see Appendix C, Sec. 2.5). Table 5-46 describes the required comparison descriptions that are part of SARU_KFG, while Table 5-47 describes the degree to which each of IBM InfoSphere and RSA Archer meet these descriptions.

Table 5-46: SARU_KFG

SARU_KFG	D1	C1	C2	C3	C4	C5	E1
Basic	X	X	X	X	X	X	X
Extended	X	X	X	X	X	X	X
High	**X**	**X**	**X**	**X**	**X**	**X**	**X**

Table 5-47: SARU_KFG Comparison

Requirement Description	IBM Guardium	RSA Archer
SARU_KFG.D1 The system developer shall provide documented administrative procedures to implement configuration management system.	Not at all	Not at all
SARU_KFG.C1 The procedures shall describe how the current version and update level for all software in the system to be documented.	Not at all	Not at all
SARU_KFG.C2 The procedures shall describe how the current configuration of all components in the system must be documented.	Not at all	Not at all
SARU_KFG.C3 The procedures shall describe how the periodic inspection of the documentation is consistent with the system to be implemented by the operating staff.	Not at all	Not at all
SARU_KFG.C4 The procedures shall describe how any changes to the system software and configuration shall be decided and documented before implementation.	Not at all	Not at all

Requirement Description	IBM Guardium	RSA Archer
SARU_KFG.C5 The procedures shall describe how changing decisions are documented and show that they should include the reason, purpose and document exactly what changes will be implemented.	Not at all	Not at all
SARU_KFG.E1 The evaluator shall verify that the information in the dossier meets all requirements for content and presentation.	Not at all	Not at all

5.6.6 SARU_UTB – Security training for users

The objective of SARU_UTB is to confirm that the security training is provided for the system users [1] (see Appendix C, Sec. 2.5). Table 5-48 describes the required comparison descriptions that are part of SARU_UTB, while Table 5-49 describes the degree to which each of IBM InfoSphere and RSA Archer meet these descriptions.

Table 5-48: SARU_UTB

SARU_UTB	D1	D2	C1	C2	C3	C4	C5	E1
Basic	X	X	X	X	X	X	X	X
Extended	X	X	X	X	X	X	X	X
High	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**

Table 5-49: SARU_UTB Comparison

Requirement Description	IBM Guardium	RSA Archer
SARU_UTB.D1 The system developer shall provide a basis for training.	Completely (IBM Security offers courses and guides for uses training.)	Completely (RSA offers training for end users of RSA Archer.)
SARU_UTB.D2 The system developer shall provide procedures for user training.	Completely	Completely
SARU_UTB.C1 Training documentation shall be provided for all types of system users.	Completely (The installation and configuration of IBM InfoSphere Guardium includes the technical training for assigned administrators and users.)	Completely (RSA Archer Training Service)

Requirement Description	IBM Guardium	RSA Archer
SARU_UTB.C2 Training documentation shall include descriptions of how users should report security-related incidents and the types of incidents that should be reported.	Completely	Completely
SARU_UTB.C3 Training documentation shall for each type of user specify conditions such as previous knowledge.	Not at all	Not at all
SARU_UTB.C4 The procedures for training shall specify how training is conducted and how the completed training means that users understand the use and their role in maintaining the system security.	Completely	Completely
SARU_UTB.E1 The evaluator shall verify that the information in the dossier meets all requirements for content and presentation.	Not at all	Not at all

5.7 SATS - System integration test

SATS – System integration test [1] (see Appendix C, Sec. 2.6) is used when confirming that the security functionality of a system works properly, and that the security features are not circumvented.

This class consists of the following four assurance requirements that will be compared to IBM Guardium and RSA Archer: SATS_TTK, SATS_FUN, SATS_ANG, and SATS_EVL.

5.7.1 SATS_TTK – Test coverage

The objective of SATS_TTK [1] (see Appendix C, Sec. 2.6) is to verify that the security functional requirements of a system and system components are tested properly. Table 5-50 describes the required comparison descriptions that are part of SATS_TTK, while Table 5-51 describes the degree to which each of IBM InfoSphere and RSA Archer meet these descriptions.

Table 5-50: SATS_TTK

SATS_TTK	D1	C1	C2	C3	C4	C5	E1
Basic	X	X					X
Extended	X	X	X	X			X
High	**X**	**X**	**X**	**X**	**X**	**X**	**X**

Table 5-51: SATS_TTK Comparison

Requirement Description	IBM Guardium	RSA Archer
SATS_TTK.D1 The system developer shall provide an analysis of the test coverage for functional and attacker tests.	Not at all	Not at all
SATS_TTK.C1 The analysis shall include a justification for the performance of the functional tests and why attacker tests are considered sufficient and coverall system security features.	Not at all	Not at all
SATS_TTK.C2 The analysis shall show how the test cases in the test documentation are consistent with the security functional requirements, security functions and components as described in the design documentation.	Not at all	Not at all
SATS_TTK.C3 The analysis shall show that all the requirement components in all functional safety requirements are tested.	Not at all	Not at all
SATS_TTK.C4 The analysis shall show that all of the system's security functions are tested in all security-relevant components that implement them.	Not at all	Not at all
SATS_TTK.C5 The analysis shall demonstrate that all security-relevant components of security functionality of the system are tested for all component interfaces.	Not at all	Not at all
SATS_TTK.E1 The evaluator shall verify that the information in the dossier meets all requirements for content and presentation.	Not at all	Not at all

5.7.2 SATS_FUN – Functional tests

The objective of SATS_FUN SATS_TTK [1] (see Appendix C, Sec. 2.6) is to confirm that the functional tests for the security functionality are implemented. Table 5-52 describes the required comparison descriptions that are part of SATS_FUN, while Table 5-53 describes the degree to which each of IBM InfoSphere and RSA Archer meet these descriptions.

Table 5-52: SATS_FUN

SATS_FUN	D1	D2	D3	C1	C2	C3	C4	C5	E1
Basic	X	X		X	X	X	X	X	X
Extended	X	X	X	X	X	X	X	X	X
High	X	X	X	X	X	X	X	X	X

Table 5-53: SATS_FUN Comparison

Requirement Description	IBM Guardium	RSA Archer
SATS_FUN.D1 The system developer shall test the system and produce the test documentation.	Not at all	Not at all
SATS_FUN.D2 The system developer shall provide a test report.	Not at all	Not at all
SATS_FUN.D3 The system developer shall provide test documentation.	Not at all	Not at all
SATS_FUN.C1 The test report shall include description of how the tests were carried out (testing the overall performance as well as any complaints regarding the outcome of the tests).	Not at all	Not at all
SATS_FUN.C2 The test documentation shall consist of test plans, expected results and actual results.	Not at all	Not at all
SATS_FUN.C3 Test plans shall describe the tests to be carried out, and the scenario for each test. The descriptions should be so detailed that the tests can be reproduced.	Not at all	Not at all

Requirement Description	IBM Guardium	RSA Archer
SATS_FUN.C4 The expected result shall describe how a successful test results can be identified and distinguished from a non-successful test results. This should be done for each test case.	Not at all	Not at all
SATS_FUN.C5 The actual test results shall be consistent with the expected test results.	Not at all	Not at all
SATS_FUN.E1 The evaluator shall verify that the information in the dossier meets all requirements for content and presentation.	Not at all	Not at all

5.7.3 SATS_ANG – Attacker tests

The objective of SATS_ANG [1] (see Appendix C, Sec. 2.6) is to ensure that the attacker tests, that focus on demonstrating that security functionality of components is present and works properly, are implemented in the system. Table 5-54 describes the required comparison descriptions that are part of SATS_ANG, while Table 5-55 describes the degree to which each of IBM InfoSphere and RSA Archer meet these descriptions.

Table 5-54: SATS_ANG

SATS_ANG	D1	D2	D3	C1	C2	C3	C4	C5	E1
Basic	X	X		X	X	X	X	X	X
Extended	X	X	X	X	X	X	X	X	X
High	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**

Table 5-55: SATS_ANG Comparison

Requirement Description	IBM Guardium	RSA Archer
SATS_ANG.D1 The system developer shall test the system and produce the test documentation.	Not at all	Not at all
SATS_ANG.D2 The system developer shall provide a test report.	Not at all	Not at all
SATS_ANG.D3 The system developer shall provide test documentation.	Not at all	Not at all

Requirement Description	IBM Guardium	RSA Archer
SATS_ANG.C1 The test report shall include description of how the tests were carried out (testing the overall performance as well as any complaints regarding the outcome of the tests).	Not at all	Not at all
SATS_ANG.C2 The test documentation shall consist of test plans, expected results and actual results.	Not at all	Not at all
SATS_ANG.C3 Test plans shall describe the tests to be carried out, and the scenario for each test. The descriptions should be so detailed that the tests can be reproduced.	Not at all	Not at all
SATS_ANG.C4 The expected result shall describe how a successful test results can be identified and distinguished from a non-successful test results. This should be done for each test case.	Not at all	Not at all
SATS_ANG.C5 The actual test results shall be consistent with the expected test results.	Not at all	Not at all
SATS_ANG.E1 The evaluator shall verify that the information in the dossier meets all requirements for content and presentation.	Not at all	Not at all

5.7.4 SATS_EVL – Evaluation testing

The objective of SATS_EVL [1] (see Appendix C, Sec. 2.6) is to analyze the tests performed by the system evaluator. Table 5-56 describes the required comparison descriptions that are part of SATS_EVL, while Table 5-57 describes the degree to which each of IBM InfoSphere and RSA Archer meet these descriptions.

Table 5-56: SATS_EVL

SATS_EVL	D1	D2	C1	E1	E2	E3	E4
Basic	X	X	X	X	X		
Extended	X	X	X	X	X	X	X
High	**X**	**X**	**X**	**X**	**X**	**X**	**X**

Table 5-57: SATS_EVL Comparison

Requirement Description	IBM Guardium	RSA Archer
SATS_EVL.D1 The system developer shall provide system testing.	Not at all	Not at all
SATS_EVL.D2 The system developer shall provide corresponding set of test resources as those used by the systems developer for the functional testing.	Not at all	Not at all
SATS_EVL.C1 The IT system shall be in a testable condition.	Not at all	Not at al
SATS_EVL.E1 The evaluator shall verify that the information in the dossier meets all requirements for content and presentation.	Not at all	Not at all
SATS_EVL.E2 The evaluator shall, if it deems necessary, repeat a representative number of systems developer's tests to confirm the system developer's test results for these test cases.	Not at all	Not at all
SATS_EVL.E3 The evaluator shall analyze the system developer's test cases and complement them with its own test cases.	Not at all	Not at all
SATS_EVL.E4 The evaluator shall implement its own test cases, document the results and confirm that the system works according to specifications.	Not at all	Not at all

5.8 SARA - Risk analysis and vulnerability assessment

SARA – Risk analysis and vulnerability assessment [1] (see Appendix C, Sec. 2.7) is used when identifying and analyzing abnormalities, weaknesses, and risks in the system.

This class consists of the following three assurance requirements that will be compared to IBM Guardium and RSA Archer: SARA_AVV, SARA_SBH, and SARA_RRA.

5.8.1 SARA_AVV – Deviation analysis

The objective of SARA_AVV is to confirm that security-related deviations in the system are recognized and defined in order to take the appropriate measures [1] (see Appendix C, Sec. 2.7). Table 5-58 describes the required comparison descriptions that are part of SARA_AVV, while Table 5-59 describes the degree to which each of IBM InfoSphere and RSA Archer meet these descriptions.

Table 5-58: SARA_AVV

SARA_AVV	D1	C1	C2	C3	C4	C5	E1
Basic	X	X	X	X	X	X	X
Extended	X	X	X	X	X	X	X
High	**X**	**X**	**X**	**X**	**X**	**X**	**X**

Table 5-59: SARA_AVV Comparison

Requirement Description	IBM Guardium	RSA Archer
SARA_AVV.D1 The system developer shall provide a deviation analysis.	Completely	Completely
SARA_AVV.C1 Deviation analysis shall include all deviations from the approved configuration of all system security-relevant components.	Completely	Completely
SARA_AVV.C2 Deviation analysis shall include all deviations from the approval of the intended use of all the system's security-relevant components.	Completely	Completely
SARA_AVV.C3 Deviation analysis shall include all deviations from the approval of the assumptions about the system design for all system's security-relevant components.	Completely	Completely
SARA_AVV.C4 Deviation analysis shall for any deviation show what impact it has and how it has been handled.	Completely	Completely
SARA_AVV.C5 Deviation analysis shall show that the measures taken to deal with the deviations are effective.	Completely	Completely

Requirement Description	IBM Guardium	RSA Archer
SARA_AVV.E1 The evaluator shall verify that the information in the dossier meets all requirements for content and presentation.	Not at all	Not at all

5.8.2 SARA_SBH – Vulnerability analysis

The objective of SARA_SBH is to confirm that the vulnerability analysis is performed for the system [1] (see Appendix C, Sec. 2.7). Table 5-60 describes the required comparison descriptions that are part of SARA_SBH, while Table 5-61 describes the degree to which each of IBM InfoSphere and RSA Archer meet these descriptions.

Table 5-60: SARA_SBH

SARA_SBH	D1	C1	E1	E2	E3	E4	E5	E6	E7
Basic	X	X	X	X	X	X			
Extended	X	X	X	X	X		X		X
High	**X**	**X**	**X**	**X**	**X**			**X**	**X**

Table 5-61: SARA_SBH Comparison

Requirement Description	IBM Guardium	RSA Archer
SARA_SBH.D1 The system developer shall provide system testing.	Not at all	Not at all
SARA_SBH.C1 The IT system shall be in a testable condition.	Not at all	Not at all
SARA_SBH.E1 The evaluator shall verify that the information in the supplier's documentation is sufficient to perform a thorough vulnerability assessment of the entire system.	Not at all	Not at all
SARA_SBH.E2 The evaluator shall use available sources to supplement supplier documentation, such as audience vulnerability information.	Not at all	Not at all

Requirement Description	IBM Guardium	RSA Archer
SARA_SBH.E3 The evaluator shall analyze, using the supplier's documentation and other available information, the system components and interfaces and map their dependencies in order to identify the attack surface and potential weak points in the architecture.	Not at all	Not at all
SARA_SBH.E6 Evaluator shall carry out independent, methodical and semi-formal vulnerability analysis of the system based on all available information and experience to identify potential vulnerabilities in the system.	Not at all	Not at all
SARA_SBH.E7 Evaluation shall conduct practical tests of the system to determine whether potential vulnerabilities can be exploited in the intended use of the system.	Not at all	Not at all

5.8.3 SARA_RRA – Residual risk analysis

The objective of SARA_RRA is to confirm that the residual risk analysis is performed for the system [1] (see Appendix C, Sec. 2.7). Table 5-62 describes the required comparison descriptions that are part of SARA_RRA, while Table 5-63 describes the degree to which each of IBM InfoSphere and RSA Archer meet these descriptions.

Table 5-62: SARA_RRA

SARA_RRA	E1	E2	E3
Basic	X	X	X
Extended	X	X	X
High	**X**	**X**	**X**

Table 5-63: SARA_RRA Comparison

Requirement Description	IBM Guardium	RSA Archer
SARA_RRA.E1 The evaluator shall verify that all other evaluating activities are completed successfully.	Not at all	Not at all
SARA_RRA.E2 The evaluator shall implement the residual risk analysis to identify remaining uncertainties about the system's IT security skills.	Not at all	Not at all
SARA_RRA.E3 Evaluator shall document the results of the residual risk analysis in a form and language that is clear and gives the intended recipient the basis for decisions on accreditation.	Not at all	Not at all

5.9 Summary of Comparisons

This section summarizes the requirements that were analyzed in the previous sections in order to select the most suitable security management solution.

Table 5-64 summarizes the findings from the previous sections. It is evident that IBM InfoSphere Guardium *completely* satisfies more requirements than RSA Archer. In addition, the number of requirements that are *not at all* satisfied is smaller for IBM InfoSphere Guardium. Both solutions have the same number of partially fulfilled requirements. Hence, IBM InfoSphere Guardium is selected as the most suitable security management solution for the Swedish Armed Forces.

It must be noted that a large number of requirements that are not met for both solutions is due to the lack of detailed documentation available on the Internet available for comparison with the assurance requirements. Neither IBM nor RSA has produced their documentation according to the KSF v3.1 requirements and hence many requirements could not be fulfilled. Furthermore, it is important to realize that some requirements were classified as not fulfilled because the supporting documentation could not be found. However, it might be the case that a specific requirement is actually fulfilled, but the supporting documentation was unavailable via the Internet.

As one might expect, some of the requirements that were classified as *not at all* or *partially* fulfilled will have to be fulfilled *completely* in order for the solution to be accepted and integrated. The first step is to request IBM to produce an ITSS based on the KSF v3.1. It is the task of the Swedish Armed Forces to specify what has to be fulfilled, and IBM has to prove that the specified requirements are actually fulfilled in order to be eligible for being a supplier. Moreover, what has to be fulfilled is based on the assurance level of the solution, which is determined by using a component assurance process.

Table 5-64: Summary of requirement comparisons

Requirement	IBM InfoSphere Guardium			RSA Archer		
	Completely	Partially	Not at all	Completely	Partially	Not at all
SASS_INL	2	1	6	2	0	7
SASS_SYS	4	5	4	4	5	4
SASS_KRV	0	0	8	0	0	8
SASS_OMG	2	1	4	0	0	7
SASS_TOL	0	0	6	0	0	6
SASS_UPF	0	0	6	0	0	6
SALC_UTV	2	2	6	2	2	6
SALC_KFG	2	0	13	1	3	11
SALC_LEV	2	1	3	0	0	6
SALC_LCM	6	1	7	6	1	7
SALC_BRK	14	0	1	14	0	1
SADE_GRÄ	3	1	2	3	1	2
SADE_ARK	5	0	2	5	0	2
SADE_DFA	6	0	1	6	0	1
SADE_DES	5	1	2	5	1	2
SAOP_INS	4	0	3	4	0	3
SAOP_DOK	7	1	2	6	2	2
SAOP_BRK	5	0	6	5	0	6
SARU_ ÅTK	6	0	5	6	0	5
SARU_ATT	5	1	3	0	0	9
SARU_INT	5	1	6	5	1	6
SARU_UPD	4	0	6	4	0	6
SARU_KFG	0	0	7	0	0	7
SARU_UTB	5	0	2	5	0	2
SATS_TTK	0	0	7	0	0	7
SATS_FUN	0	0	9	0	0	9
SATS_ANG	0	0	9	0	0	9
SATS_EVL	0	0	7	0	0	7
SARA_AVV	6	0	1	6	0	1
SARA_SBH	0	0	7	0	0	7
SARA_RRA	0	0	3	0	0	3
Total	**100**	**16**	**154**	**89**	**16**	**165**

6 Component Assurance Process

The purpose of this chapter is to construct a component assurance process and explain the main concepts behind it.

Section 6.1 describes the main concepts that are necessary to understand the component assurance process. Section 6.2 proposes the component assurance process.

6.1 Concepts from the KSF v3.1

The component assurance process is defined as the process that is used when confirming a specific security-related IT component meets a specific component assurance level [1] (see Appendix A, Sec. 4.3).

Every IT system consists of IT components, and some of these components influence the security of the entire system. These security-related components either have some security function or the security function depends on them. Hence, it is important to create a process that will be used when determining the assurance level of the security-related IT components.

Every security-related IT component is also characterized by its consequence and exposure level. A consequence level describes what kind of impact a security breach regarding a certain component would have on the entire system. An exposure level describes the exposure of the component, either physically as a result of people accessing the physical equipment or logically via interfaces. The consequence and exposure level determine which assurance level the component *must* have. Moreover, the component is *approved* to a certain assurance level if it satisfies the assurance requirements that are stated by that assurance level. Table 6-1 shows the relationship between a component's assurance level and its exposure and consequence levels; e.g., a component that has the highest exposure level (E4) and the highest consequence level (K5) *must* have the highest assurance level (N4). However, in order to be admitted to that level, certain assurance requirements must be fulfilled.

Table 6-1: Relationship between component assurance levels and consequence and exposure levels (Adapted from Table 6 of [1])

	Exposure level			
Consequence level	**E1**	**E2**	**E3**	**E4**
K5	N2	N3	N4	N4
K4	N2	N2	N4	N4
K4	N2	N2	N3	N4
K2	N1	N2	N2	N3
K1	N1	N1	N1	N1

The following section explains the details of determining the consequence and exposure levels of a component.

6.2 Proposal of a Component Assurance Process

This section explains the elements of the proposed component assurance process. Figure 6-1 shows a simplified or general view of the component assurance process. There are five main activities in this process: identification of the security-related components in the system, identification of the consequence level for every security-related component that was previously identified, identification of the exposure level for every security-related component that was previously identified, identification of the assurance level for each security-related component in order to determine the level of assurance that the component *must* satisfy, and fulfillment of specific requirements for the sake of assigning a component to its identified assurance level.

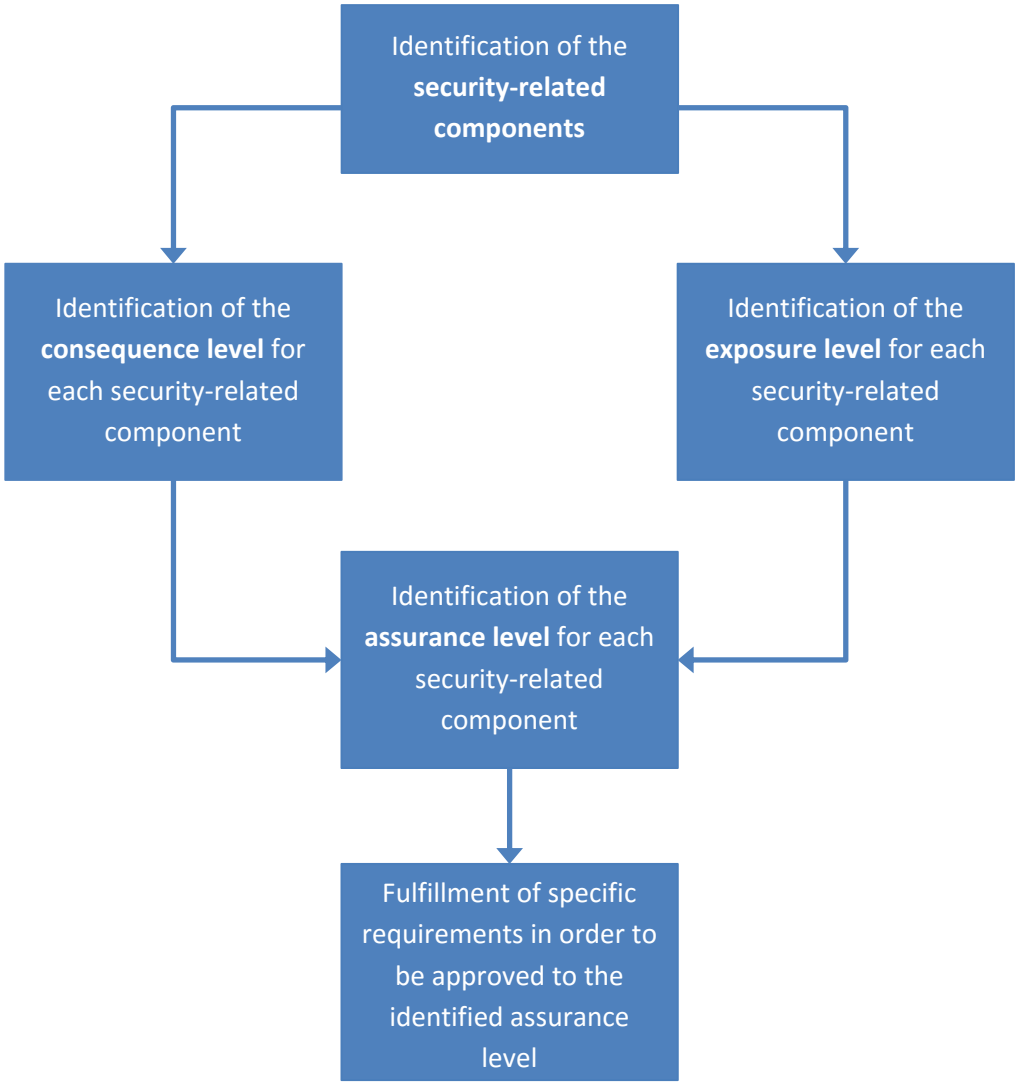

Figure 6-1: A general view of the component assurance process

6.2.1 The security-related components identification

The first element of the component assurance process is the identification of the security-related components in the system. This first step includes the following activities:

1. Identification of all components within a certain system.
2. Performing *risk identification* in order to identify the potential risks in the system.
3. Performing *risk analysis* in order to analyze the identified risks and to determine which system components are affected by these risks or which components contribute to these risks.
4. Performing risk assessment in order to prioritize the risks and security-related components.

6.2.2 The consequence level identification

The second element of the component assurance process is the identification of the consequence level. The goal of this consequence level identification is to assign one of the following consequence levels from the KSF v3.1 to a specific security-related component:

K5 – Very serious	A security breach on a component with the consequence level K5 will have an exceptionally harmful effect on a system and hence the entire organization. The consequence for the organization is long-term and represents a direct danger. A component that has a contact with the "top secret" documentation in the Swedish Armed Forces will be appointed to this level. Disclosure of information in the "top secret" documentation might cause a *very serious* damage to the Swedish Armed Forces and even their relations with other countries or foreign organizations.
K4 - Serious	A security breach on a component with the consequence level K4 will have a serious effect on the organization's capabilities and functionalities. The consequence for the organization is *not* long-term but represents a direct danger. Components that interact with the "secret" documentation in the Swedish Armed Forces will be appointed to this level. Release of information in the "secret" documentation might cause a *serious* harm to the Swedish Armed Forces and their relations with other countries or foreign organizations.
K3 – Noticeable	A component is appointed to the consequence level K4 if a security violation on it causes a noticeable effect, such as interruptions in using the services and DoS. A component that has a contact with the "confidential" documentation in the Swedish Armed Forces will be appointed to this level. Release of information in the "confidential" documentation might cause a *noticeable* harm to the Swedish Armed Forces and their relations with other countries or foreign organizations.
K2 – Mild	A security violation on a component with the consequence level K4 will have minor consequences for the organization. A component that has a contact with the "restricted" documentation in the Swedish Armed Forces will be appointed to this level. Disclosure of information in the "restricted" documentation may cause a *minor* harm to the Swedish Armed Forces and their relations with other countries or foreign organizations.
K1 – Negligible	A component is assigned to the consequence level K4 if a security violation on it has an insignificant effect.

6.2.3 The exposure level identification

The following element of the component assurance process is the identification of components' exposure levels. According to the KSF v3.1, the two types of exposures are the following:

- **Exposure caused by employees**: Employees can access the system and therefore have an effect on the system and its components. Thus, employee activity needs to be monitored by authorized personnel in order to keep track of the system exposure.
- **Exposure caused by information exchange**: The interaction between different systems and their components also increases the exposure. Thus, the information exchange between the systems and their components must be analyzed and described.

The goal of the exposure level identification is to assign one of the following consequence levels from the KSF v3.1 to a specific security-related component:

E1 – The lowest exposure level	A component is assigned to the exposure level E1 if all employees can access this component and the information that is being handled by the component. In addition, this component does not exchange information with any components of other systems.
E2	A component is assigned to the exposure level E2 if it can be accessed only by employees who are authorized to handle components with the higher consequence levels. Moreover, this component only exchanges information with the components that are assigned to higher consequence levels than its level or with components that are assigned to the same consequence level and their maximum exposure level is E2.
E3	A component is assigned to the exposure level E3 if all the people who access the component and its interfaces are security tested according to the Security Protection Ordinance [109]. In addition, this component only exchanges information with the components that are assigned to higher consequence levels than its level or with the components that are assigned to the same consequence level and their maximum exposure level is E3.
E4 – The highest exposure level	A component is assigned to the exposure level E4 if it does not satisfy the requirements of the above mentioned exposure levels.

6.2.4 Assurance level identification

After identifying the consequence and exposure levels of a specific component, it is possible to determine the assurance level required for that component. However, it is very important to emphasize that this phase only determines the assurance level that a certain component *must* satisfy and *does not assign* a component to that specific assurance level.

Table 6-1 is used when identifying an assurance level that a certain component must satisfy. As shown in the table, there are four assurance levels, starting from the lowest assurance level (N1) up to the highest level of assurance (N4).

6.2.5 Assurance level assignment

After identifying the assurance level of a particular component, it important to fulfill the following requirements in order to for the component to be assigned its identified assurance level:

N4	The component developer has to provide documentation that demonstrates that a component was developed using formal project methodology such as United States Air Force, Military Standard 1521B* [110] . The component developer has to provide documentation that shows that a component fully satisfies the assurance requirements stated in the KSF v3.1. The component developer has to provide documentation that demonstrates the security architecture of a component. The component developer has to provide documentation that explains the development plan of a component. The component developer has to provide documentation that shows how the testing of the component was conducted. The component developer must provide an ITSS including the ITSS system reference, identification of the system, identification of the version of the KSF requirements, identification of the security documentation, and the system overview. The component developer must provide a system description that describes the information handled in the system or component, the consequences of the information loss, component exposure, users of the component, and component interfaces and their purpose. The component developer must describe security requirements on the environment. The component developer must provide an interpretation of security requirements. The component developer must describe the compliance with security requirements. The component developer must provide the system development documentation. The component developer must provide the system integration documentation. The component developer must provide the explanation of acceptance criteria that is used when including a component in the system. The component developer must use a configuration management system and provide a documentation describing that system. The component developer must provide an explanation of the component delivery procedures. This documentation must describe how the accuracy of the component is protected during the delivery, and how the accuracy is verified after the receipt of the component. The component developer must establish a component life-cycle model and provide documentation describing it. The component developer must implement fault correction and provide procedures for the management of security-related deficiencies. The description of the component's interfaces must include all the interactions with the other components and their interfaces. A data flow analysis of the critical data must be provided. Design documentation must be provided. A documentation describing the preparation and installation of a component must be provided. The preparation must include activities used when verifying that a component is installed correctly. Operating and administrative documentation must be provided. Administrative procedures for the allocation and revocation of access rights must be

* This standard was retired in MIL-STD-1521B (NOTICE 3), 10 April 1995.

	provided. These procedures must describe that only authorized personnel have access rights to administrative functions. In addition, these procedures must describe that a person can be assigned access rights to only one of the following roles: administration of access control, administration of security log, and other operating administration. Moreover, only a person in charge of the administration of security logs can be granted access right to security logs. The procedures must also describe that a person can be assigned access rights to only one of the following roles: administration of identities and security attributes used for authentication, and assignment of roles and access rights to users. The quality of security attributes that are used for authentication must be controlled. Moreover, administrative procedures responsible for this must be provided. The procedures explaining security updates must be provided. The procedures for user training must be provided. Functional test documentation must be produced and a test report provided. A security-related deviation analysis must be provided. A residual risk analysis must be provided.
N3	The component developer has to provide documentation that shows that a component satisfies most of the assurance requirements stated in the KSF v3.1. The component developer has to provide documentation that shows how the testing of the component was conducted. The component developer must provide an ITSS including the ITSS system reference, identification of the system, identification of the version of the KSF requirements, identification of the security documentation, and the system overview. The component developer must provide a system description that describes the information handled in the system or component, the consequences of the information loss, component exposure, users of the component, and component interfaces and their purpose. The component developer must describe security requirements on the environment. The component developer must provide an interpretation of security requirements. The component developer must describe the compliance with security requirements. The component developer must provide the system development documentation. The component developer must provide the system integration documentation. This documentation must identify the origin of components. The component developer must provide the explanation of acceptance criteria that is used when including a component in the system. The acceptance criteria must describe how the security-related components are accepted and verified. The component developer must use a configuration management system and provide a documentation describing that system. The component developer must provide an explanation of the component delivery procedures. This documentation must describe how the accuracy of the component is protected during the delivery, and how the accuracy is verified after the receipt of the component. The component developer must establish a component life-cycle model and provide a documentation describing it. The component developer must implement fault correction and provide procedures for the management of security-related deficiencies. The description of the component's interfaces must include all the interactions with the other components and their interfaces. A data flow analysis of the critical data must be provided. Design documentation must be provided. A documentation describing the preparation and installation of a component must be provided. The preparation must include activities used when verifying that a component is installed correctly. Operating and administrative documentation must be provided.

	Administrative procedures for the allocation and revocation of access rights must be provided. These procedures must describe that only authorized personnel has access rights to administrative functions. In addition, these procedures must describe that a person can be assigned access rights to only one of the following roles: administration of access control, administration of security log, and other operating administration. Moreover, only a person in charge of the administration of security logs can be granted access right to security logs. The quality of security attributes that are used for authentication must be controlled. Moreover, administrative procedures responsible for this must be provided. The procedures explaining security updates must be provided. The procedures for user training must be provided. The procedures for user training must be provided. Functional test documentation must be produced and a test report provided. A security-related deviation analysis must be provided. A residual risk analysis must be provided.
N2	The component developer has to provide component's source code. The component developer has to provide documentation that shows how the testing of the component was conducted. The component developer has to provide documentation that confirms that security review was performed by a third party. The component developer must provide an ITSS including the ITSS system reference, identification of the system, identification of the version of the KSF requirements, identification of the security documentation, and the system overview. The component developer must provide a system description that describes the information handled in the system or component, the consequences of the information loss, component exposure, users of the component, and component interfaces and their purpose. The component developer must describe security requirements on the environment. The component developer must provide an interpretation of security requirements. The component developer must describe the compliance with security requirements. The component developer must provide the system development documentation. The component developer must provide the system integration documentation. This documentation must identify the origin of components. The component developer must provide the explanation of acceptance criteria that is used when including a component in the system. The acceptance criteria must describe how the security-related components are accepted and verified. The component developer must use a configuration management system and provide a documentation describing that system. The component developer must provide an explanation of the component delivery procedures. This documentation must describe how the accuracy of the component is protected during the delivery, and how the accuracy is verified after the receipt of the component. The component developer must establish a component life-cycle model and provide a documentation describing it. The component developer must implement fault correction and provide procedures for the management of security-related deficiencies. The description of the component's interfaces must include all the interactions with the other components and their interfaces. A data flow analysis of the critical data must be provided. Design documentation must be provided. A documentation describing the preparation and installation of a component must be provided. The preparation must include activities used when verifying that a component is installed correctly.

	Operating and administrative documentation must be provided. Administrative procedures for the allocation and revocation of access rights must be provided. These procedures must describe that only authorized personnel has access rights to administrative functions. In addition, these procedures must describe that a person can be assigned access rights to only one of the following roles: administration of access control, administration of security log, and other operating administration. Moreover, only a person in charge of the administration of security logs can be granted access right to security logs. The quality of security attributes that are used for authentication must be controlled. Moreover, administrative procedures responsible for this must be provided. The procedures explaining security updates must be provided. The procedures for user training must be provided. Functional test documentation must be produced and a test report provided. A security-related deviation analysis must be provided. A residual risk analysis must be provided.
N1	The component developer has to provide documentation that demonstrates the security function of a component. The component developer has to provide documentation that demonstrates the dependencies between the specific component and other identified components. The component developer must provide an ITSS including the ITSS system reference, identification of the system, identification of the version of the KSF requirements, identification of the security documentation, and the system overview. The component developer must provide a system description that describes the information handled in the system or component, the consequences of the information loss, component exposure, users of the component, and component interfaces and their purpose. The component developer must describe security requirements on the environment. The component developer must provide an interpretation of security requirements. The component developer must describe the compliance with security requirements. The component developer must provide an explanation of the component delivery procedures. This documentation must describe how the accuracy of the component is protected during the delivery. The component developer must implement fault correction and provide procedures for the management of security-related deficiencies. A documentation describing the preparation and installation of a component must be provided. Operating and administrative documentation must be provided. Administrative procedures for the allocation and revocation of access rights must be provided. These procedures must describe that only authorized personnel has access rights to administrative functions. The quality of security attributes that are used for authentication must be controlled. Moreover, administrative procedures responsible for this must be provided. The procedures explaining security updates must be provided. The procedures for user training must be provided. Functional test documentation must be produced. A security-related deviation analysis must be provided. A residual risk analysis must be provided.

Table 6-2 shows the relationship between the strength of assurance requirements and component assurance level. This table is a result of combining Table 5-1 and Table 6-1.

Table 6-2: Relationship between assurance requirement strength and component assurance levels

	Exposure level			
Consequence level	**E1**	**E2**	**E3**	**E4**
K5	H/N2	H/N3	H/N4	H/N4
K4	U/N2	H/N2	H/N4	H/N4
K4	U/N2	U/N2	U/N3	H/N4
K2	G/N1	U/N2	U/N2	U/N3
K1	G/N1	G/N1	G/N1	G/N1

Figure 6-2 uses Table 6-2 to summarize the link between each category of assurance requirement strength and the component assurance levels. Thus, the following can be concluded:

- If the strength of a specific requirement is *G (Ground)* then a component that must satisfy the *assurance level N1* has to fulfill this requirement in order to be assigned to the assurance level N1.
- If the strength of a specific requirement is *U (Extended)* then the components that must satisfy the *assurance levels N2 and N3* have to fulfill this requirement in order to be assigned to the assurance levels N2 and N3.
- If the strength of a specific requirement is *H (High)* then the components that must satisfy the *assurance levels N2, N3, and N4* have to fulfill this requirement in order to be assigned to the assurance levels N2, N3, and N4.

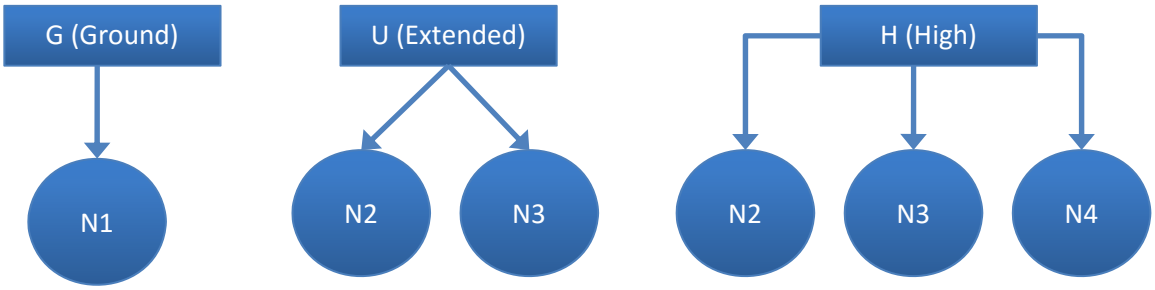

Figure 6-2: Summary of relationship between assurance requirement strength and component assurance levels

It is possible to determine which assurance requirements each component has to satisfy in order to be assigned to its identified assurance level by looking at the requirement strength tables from Chapter 5. For example, by looking at Table 5-60, we can see that the assurance requirement SARA_SBH.E4 is of basic strength, which implies that a component that must satisfy assurance level N1 has to fulfill this requirement in order to be assigned to the assurance level N1. Moreover, the assurance requirement SARA_SBH.E7 is of both extended and high strength, and this implies that components, that must satisfy the assurance levels N2, N3, and N4, have to fulfill this requirement in order to be assigned to these assurance levels.

Table 6-3 shows a checklist that is used when checking which requirements have to be satisfied by a certain component that has been identified to assign it to a certain component assurance level. For example, it is clear that a component that has to be assigned to the assurance level N1, has to meet the smallest number of requirements. This is very straightforward because the assurance level N1 represents the lowest level of assurance. However, it might be time-consuming to go through this checklist for each component, hence in most cases the summarized requirements list from the beginning of the section will be used. Nevertheless, this checklist is very useful in order to understand the relationship between the component assurance levels and assurance requirements that are stated in the KSF v3.1.

Different symbols are used in the Table 6-3 to denote the four component assurance levels, and the filled shading is used to differentiate between classes of assurance requirements. The square symbol (■) is used to denote the assurance requirements that must be fulfilled in order for a specific component to be approved to the assurance level N1. The diamond symbol (◆) is used to denote the assurance requirements that must be fulfilled in order for a specific component to be approved to the assurance level N2. The cross symbol (✦) is used to denote the assurance requirements that must be fulfilled in order for a specific component to be approved to the assurance level N3. Lastly, the star symbol (★) is used to denote the assurance requirements that must be fulfilled in order for a specific component to be approved to the assurance level N4.

Table 6-3: Assurance requirements checklist

Assurance Requirement	Assurance Requirement Strength			Component Assurance level			
	G (Ground)	U (Extended)	H (High)	N1	N2	N3	N4
SASS_INL.D1	X	X	X	■	◆	✦	★
SASS_INL.C1	X	X	X	■	◆	✦	★
SASS_INL.C2	X	X	X	■	◆	✦	★
SASS_INL.C3	X	X	X	■	◆	✦	★
SASS_INL.C4	X	X	X	■	◆	✦	★
SASS_INL.C5	X	X	X	■	◆	✦	★
SASS_INL.C6	X	X	X	■	◆	✦	★
SASS_INL.C7	X	X	X	■	◆	✦	★
SASS_INL.E1	X	X	X	■	◆	✦	★
SASS_SYS.D1	X	X	X	■	◆	✦	★
SASS_SYS.C1	X	X	X	■	◆	✦	★
SASS_SYS.C2	X	X	X	■	◆	✦	★
SASS_SYS.C3	X	X	X	■	◆	✦	★
SASS_SYS.C4	X	X	X	■	◆	✦	★
SASS_SYS.C5	X	X	X	■	◆	✦	★
SASS_SYS.C6	X	X	X	■	◆	✦	★
SASS_SYS.C7	X	X	X	■	◆	✦	★

SASS_SYS.C8	X	X	X	■	◆	✦	★
SASS_SYS.C9	X	X	X	■	◆	✦	★
SASS_SYS.C10	X	X	X	■	◆	✦	★
SASS_SYS.C11	X	X	X	■	◆	✦	★
SASS_SYS.E1	X	X	X	■	◆	✦	★
SASS_KRV.D1	X	X	X	■	◆	✦	★
SASS_KRV.C1	X	X	X	■	◆	✦	★
SASS_KRV.C2	X	X	X	■	◆	✦	★
SASS_KRV.C3	X	X	X	■	◆	✦	★
SASS_KRV.C4	X	X	X	■	◆	✦	★
SASS_KRV.C5	X	X	X	■	◆	✦	★
SASS_KRV.C6	X	X	X	■	◆	✦	★
SASS_KRV.E1	X	X	X	■	◆	✦	★
SASS_OMG.D1	X	X	X	■	◆	✦	★
SASS_OMG.C1	X	X	X	■	◆	✦	★
SASS_OMG.C2	X	X	X	■	◆	✦	★
SASS_OMG.C3	X	X	X	■	◆	✦	★
SASS_OMG.C4	X	X	X	■	◆	✦	★
SASS_OMG.C5	X	X	X	■	◆	✦	★
SASS_OMG.E1	X	X	X	■	◆	✦	★
SASS_TOL.D1	X	X	X	■	◆	✦	★
SASS_TOL.C1	X	X	X	■	◆	✦	★
SASS_TOL.C2	X	X	X	■	◆	✦	★
SASS_TOL.C3	X	X	X	■	◆	✦	★
SASS_TOL.C4	X	X	X	■	◆	✦	★
SASS_TOL.E1	X	X	X	■	◆	✦	★
SASS_UPF.D1	X	X	X	■	◆	✦	★
SASS_UPF.C1	X	X	X	■	◆	✦	★
SASS_UPF.C2	X	X	X	■	◆	✦	★
SASS_UPF.C3	X	X	X	■	◆	✦	★
SASS_UPF.C4	X	X	X	■	◆	✦	★
SASS_UPF.E1	X	X	X	■	◆	✦	★
SALC_UTV.D1		X	X		◆	✦	★
SALC_UTV.D2		X	X		◆	✦	★

SALC_UTV.D3		X	X		◆	✦	★
SALC_UTV.D4		X	X		◆	✦	★
SALC_UTV.C1		X	X		◆	✦	★
SALC_UTV.C2		X	X		◆	✦	★
SALC_UTV.C3		X			◆	✦	★
SALC_UTV.C4		X			◆	✦	★
SALC_UTV.C5			X		◆	✦	★
SALC_UTV.C6			X		◆	✦	★
SALC_UTV.E1		X	X		◆	✦	★
SALC_UTV.E2		X	X		◆	✦	★
SALC_KFG.D1		X	X		◆	✦	★
SALC_KFG.D2		X	X		◆	✦	★
SALC_KFG.D3		X	X		◆	✦	★
SALC_KFG.C1		X	X		◆	✦	★
SALC_KFG.C2		X	X		◆	✦	★
SALC_KFG.C3		X	X		◆	✦	★
SALC_KFG.C4		X	X		◆	✦	★
SALC_KFG.C5		X	X		◆	✦	★
SALC_KFG.C6		X	X		◆	✦	★
SALC_KFG.C7		X	X		◆	✦	★
SALC_KFG.C8		X	X		◆	✦	★
SALC_KFG.C9		X	X		◆	✦	★
SALC_KFG.C10			X		◆	✦	★
SALC_KFG.E1		X	X		◆	✦	★
SALC_KFG.E2		X	X		◆	✦	★
SALC_LEV.D1	X	X	X	■	◆	✦	★
SALC_LEV.D2	X	X	X	■	◆	✦	★
SALC_LEV.C1	X	X	X	■	◆	✦	★
SALC_LEV.C2	X	X	X	■	◆	✦	★
SALC_LEV.C3		X	X		◆	✦	★
SALC_LEV.E1	X	X	X	■	◆	✦	★
SALC_LCM.D1		X	X		◆	✦	★
SALC_LCM.D2		X	X		◆	✦	★
SALC_LCM.C1		X	X		◆	✦	★

SALC_LCM.C2		X	X		◆	✦	★
SALC_LCM.C3		X	X		◆	✦	★
SALC_LCM.C4		X	X		◆	✦	★
SALC_LCM.C5		X	X		◆	✦	★
SALC_LCM.C6		X	X		◆	✦	★
SALC_LCM.C7		X	X		◆	✦	★
SALC_LCM.C8		X	X		◆	✦	★
SALC_LCM.C9			X		◆	✦	★
SALC_LCM.C10			X		◆	✦	★
SALC_LCM.E1		X	X		◆	✦	★
SALC_LCM.E2		X	X		◆	✦	★
SALC_BRK.D1	X	X	X	■	◆	✦	★
SALC_BRK.D2	X	X	X	■	◆	✦	★
SALC_BRK.D3	X	X	X	■	◆	✦	★
SALC_BRK.D4	X	X	X	■	◆	✦	★
SALC_BRK.C1	X	X	X	■	◆	✦	★
SALC_BRK.C2	X	X	X	■	◆	✦	★
SALC_BRK.C3	X	X	X	■	◆	✦	★
SALC_BRK.C4	X	X	X	■	◆	✦	★
SALC_BRK.C5	X	X	X	■	◆	✦	★
SALC_BRK.C6	X	X	X	■	◆	✦	★
SALC_BRK.C7	X	X	X	■	◆	✦	★
SALC_BRK.C8	X	X	X	■	◆	✦	★
SALC_BRK.C9	X	X	X	■	◆	✦	★
SALC_BRK.C10	X	X	X	■	◆	✦	★
SALC_BRK.E1	X	X	X	■	◆	✦	★
SADE_GRÄ.D1		X	X		◆	✦	★
SADE_GRÄ.C1		X	X		◆	✦	★
SADE_GRÄ.C2		X	X		◆	✦	★
SADE_GRÄ.C3		X	X		◆	✦	★
SADE_GRÄ.C4		X	X		◆	✦	★
SADE_GRÄ.E1		X	X		◆	✦	★
SADE_ARK.D1		X	X		◆	✦	★
SADE_ARK.C1		X	X		◆	✦	★

SADE_ARK.C2		X	X		◆	✦	★
SADE_ARK.C3		X	X		◆	✦	★
SADE_ARK.E1		X	X		◆	✦	★
SADE_ARK.E2		X	X		◆	✦	★
SADE_DFA.D1		X	X		◆	✦	★
SADE_DFA.C1		X	X		◆	✦	★
SADE_DFA.C2		X	X		◆	✦	★
SADE_DFA.C3		X	X		◆	✦	★
SADE_DFA.C4		X	X		◆	✦	★
SADE_DFA.C5			X		◆	✦	★
SADE_DFA.E1		X	X		◆	✦	★
SADE_DES.D1		X	X		◆	✦	★
SADE_DES.C1		X	X		◆	✦	★
SADE_DES.C2		X	X		◆	✦	★
SADE_DES.C3		X	X		◆	✦	★
SADE_DES.C4		X	X		◆	✦	★
SADE_DES.C5		X	X		◆	✦	★
SADE_DES.C6			X		◆	✦	★
SADE_DES.E1		X	X		◆	✦	★
SAOP_INS.D1	X	X	X	■	◆	✦	★
SAOP_INS.C1	X	X	X	■	◆	✦	★
SAOP_INS.C2	X	X	X	■	◆	✦	★
SAOP_INS.C3	X	X	X	■	◆	✦	★
SAOP_INS.C4		X	X		◆	✦	★
SAOP_INS.E1	X	X	X	■	◆	✦	★
SAOP_INS.E2		X	X		◆	✦	★
SAOP_DOK.D1	X	X	X	■	◆	✦	★
SAOP_DOK.C1	X	X	X	■	◆	✦	★
SAOP_DOK.C2	X	X	X	■	◆	✦	★
SAOP_DOK.C3	X	X	X	■	◆	✦	★
SAOP_DOK.C4	X	X	X	■	◆	✦	★
SAOP_DOK.C5	X	X	X	■	◆	✦	★
SAOP_DOK.C6	X	X	X	■	◆	✦	★
SAOP_DOK.C7	X	X	X	■	◆	✦	★

SAOP_DOK.C8	X	X	X	■	◆	✦	★
SAOP_DOK.E1	X	X	X	■	◆	✦	★
SAOP_BRK.D1	X	X	X	■	◆	✦	★
SAOP_BRK.D2	X	X	X	■	◆	✦	★
SAOP_BRK.C1	X	X	X	■	◆	✦	★
SAOP_BRK.C2	X	X	X	■	◆	✦	★
SAOP_BRK.C3	X	X	X	■	◆	✦	★
SAOP_BRK.C4	X	X	X	■	◆	✦	★
SAOP_BRK.C5	X	X	X	■	◆	✦	★
SAOP_BRK.C6	X	X	X	■	◆	✦	★
SAOP_BRK.C7	X	X	X	■	◆	✦	★
SAOP_BRK.C8	X	X	X	■	◆	✦	★
SAOP_BRK.E1	X	X	X	■	◆	✦	★
SARU_ ÅTK.D1	X	X	X	■	◆	✦	★
SARU_ ÅTK.C1	X	X	X	■	◆	✦	★
SARU_ ÅTK.C2	X	X	X	■	◆	✦	★
SARU_ ÅTK.C3	X	X	X	■	◆	✦	★
SARU_ ÅTK.C4	X	X	X	■	◆	✦	★
SARU_ ÅTK.C5	X	X	X	■	◆	✦	★
SARU_ ÅTK.C6		X	X		◆	✦	★
SARU_ ÅTK.C7		X	X		◆	✦	★
SARU_ ÅTK.C8			X		◆	✦	★
SARU_ ÅTK.C9		X	X		◆	✦	★
SARU_ ÅTK.E1	X	X	X	■	◆	✦	★
SARU_ATT.D1	X	X	X	■	◆	✦	★
SARU_ATT.C1	X	X	X	■	◆	✦	★
SARU_ATT.C2	X	X	X	■	◆	✦	★
SARU_ATT.C3	X	X	X	■	◆	✦	★
SARU_ATT.C4	X	X	X	■	◆	✦	★
SARU_ATT.C5	X	X	X	■	◆	✦	★
SARU_ATT.C6	X	X	X	■	◆	✦	★
SARU_ATT.C7	X	X	X	■	◆	✦	★
SARU_ATT.E1	X	X	X	■	◆	✦	★
SARU_INT.D1	X	X	X	■	◆	✦	★

SARU_INT.C1	X	X	X	■	◆	✦	★
SARU_INT.C2	X	X	X	■	◆	✦	★
SARU_INT.C3	X	X	X	■	◆	✦	★
SARU_INT.C4	X	X	X	■	◆	✦	★
SARU_INT.C5	X	X	X	■	◆	✦	★
SARU_INT.C6	X	X	X	■	◆	✦	★
SARU_INT.C7	X	X	X	■	◆	✦	★
SARU_INT.C8		X	X		◆	✦	★
SARU_INT.C9		X	X		◆	✦	★
SARU_INT.C10	X	X	X	■	◆	✦	★
SARU_INT.E1	X	X	X	■	◆	✦	★
SARU_UPD.D1	X	X	X	■	◆	✦	★
SARU_UPD.C1	X	X	X	■	◆	✦	★
SARU_UPD.C2	X	X	X	■	◆	✦	★
SARU_UPD.C3	X	X	X	■	◆	✦	★
SARU_UPD.C4	X	X	X	■	◆	✦	★
SARU_UPD.C5	X	X	X	■	◆	✦	★
SARU_UPD.C6	X	X	X	■	◆	✦	★
SARU_UPD.C7	X	X	X	■	◆	✦	★
SARU_UPD.C8	X	X	X	■	◆	✦	★
SARU_UPD.E1	X	X	X	■	◆	✦	★
SARU_KFG.D1	X	X	X	■	◆	✦	★
SARU_KFG.C1	X	X	X	■	◆	✦	★
SARU_KFG.C2	X	X	X	■	◆	✦	★
SARU_KFG.C3	X	X	X	■	◆	✦	★
SARU_KFG.C4		X	X		◆	✦	★
SARU_KFG.C5		X	X		◆	✦	★
SARU_KFG.E1	X	X	X	■	◆	✦	★
SARU_UTB.D1	X	X	X	■	◆	✦	★
SARU_UTB.D2	X	X	X	■	◆	✦	★
SARU_UTB.C1	X	X	X	■	◆	✦	★
SARU_UTB.C2	X	X	X	■	◆	✦	★
SARU_UTB.C3	X	X	X	■	◆	✦	★
SARU_UTB.C4	X	X	X	■	◆	✦	★

SARU_UTB.C5	X	X	X	■	◆	✦	★
SARU_UTB.E1	X	X	X	■	◆	✦	★
SATS_TTK.D1	X	X	X	■	◆	✦	★
SATS_TTK.C1	X	X	X	■	◆	✦	★
SATS_TTK.C2		X	X		◆	✦	★
SATS_TTK.C3		X	X		◆	✦	★
SATS_TTK.C4			X		◆	✦	★
SATS_TTK.C5			X		◆	✦	★
SATS_TTK.E1	X	X	X	■	◆	✦	★
SATS_FUN.D1	X	X	X	■	◆	✦	★
SATS_FUN.D2	X	X	X	■	◆	✦	★
SATS_FUN.D3		X	X		◆	✦	★
SATS_FUN.C1	X	X	X	■	◆	✦	★
SATS_FUN.C2	X	X	X	■	◆	✦	★
SATS_FUN.C3	X	X	X	■	◆	✦	★
SATS_FUN.C4	X	X	X	■	◆	✦	★
SATS_FUN.C5	X	X	X	■	◆	✦	★
SATS_FUN.E1	X	X	X	■	◆	✦	★
SATS_ANG.D1	X	X	X	■	◆	✦	★
SATS_ANG.D2	X	X	X	■	◆	✦	★
SATS_ANG.D3		X	X		◆	✦	★
SATS_ANG.C1	X	X	X	■	◆	✦	★
SATS_ANG.C2	X	X	X	■	◆	✦	★
SATS_ANG.C3	X	X	X	■	◆	✦	★
SATS_ANG.C5	X	X	X	■	◆	✦	★
SATS_ANG.C5	X	X	X	■	◆	✦	★
SATS_ANG.E1	X	X	X	■	◆	✦	★
SATS_EVL.D1	X	X	X	■	◆	✦	★
SATS_EVL.D2	X	X	X	■	◆	✦	★
SATS_EVL.C1	X	X	X	■	◆	✦	★
SATS_EVL.E1	X	X	X	■	◆	✦	★
SATS_EVL.E2	X	X	X	■	◆	✦	★
SATS_EVL.E3		X	X		◆	✦	★
SATS_EVL.E4		X	X		◆	✦	★

SARA_AVV.D1	X	X	X	■	◆	✦	★
SARA_AVV.C1	X	X	X	■	◆	✦	★
SARA_AVV.C2	X	X	X	■	◆	✦	★
SARA_AVV.C3	X	X	X	■	◆	✦	★
SARA_AVV.C4	X	X	X	■	◆	✦	★
SARA_AVV.C5	X	X	X	■	◆	✦	★
SARA_AVV.E1	X	X	X	■	◆	✦	★
SARA_SBH.D1	X	X	X	■	◆	✦	★
SARA_SBH.C1	X	X	X	■	◆	✦	★
SARA_SBH.E1	X	X	X	■	◆	✦	★
SARA_SBH.E2	X	X	X	■	◆	✦	★
SARA_SBH.E3	X	X	X	■	◆	✦	★
SARA_SBH.E4	X			■		✦	★
SARA_SBH.E5		X			◆	✦	★
SARA_SBH.E6			X		◆	✦	★
SARA_SBH.E7		X	X		◆	✦	★
SARA_RRA.E1	X	X	X	■	◆	✦	★
SARA_RRA.E2	X	X	X	■	◆	✦	★
SARA_RRA.E3	X	X	X	■	◆	✦	★

If a component cannot meet all of the requirements that are needed for that component to be assigned to a certain component assurance level, then the developer must explain why the introduction of this component does *not* jeopardize the security of the organization.

According to the directions from the Swedish Armed Forces, IBM InfoSphere Guardium is in this thesis regarded as a component with exposure level E3 and consequence level K4. Thus, by looking at the Table 6-1, it can be concluded that this product must be assigned to the component assurance level N4.

7 Conclusions and Future work

This chapter provides the reader with the discussion of conclusions, limitations, and reflections. Furthermore, some future work is suggested.

Section 7.1 discusses the fulfillment of the stated goals, gained insights, and suggestions for others work in this area. Section 7.2 examines the limitations encountered during this research and the limitations of the results. Section 7.3 discusses future work and gives suggestions to someone who might build upon this work. Section 7.4 discusses the relevant ethical, social, and sustainability aspects of the work.

7.1 Conclusions

The first goal of this master's thesis project was to perform detailed security management market research and select the two leading solutions. Three security management areas were analyzed, and the two leading solutions that were selected are IBM InfoSphere Guardium and RSA Archer.

Comparing these two leading solutions with the KSF v3.1 and its assurance requirements was the second goal. The documentation concerning IBM InfoSphere Guardium and RSA Archer was compared with the assurance requirements stated in the KSF v3.1.

The third goal was selection of the solution that meets most of the requirements for further study and proposal new functionalities for this solution. The solution that meets the most assurance requirements is IBM InfoSphere Guardium and hence this solution was selected. Moreover, the assurance level of this solution was identified and the assurance requirements that need to be fulfilled can be presented to the developer(s).

The final and most significant goal of this master's thesis project was the construction of a component assurance process. The process consisting of five phases was constructed and used to determine the requirements that need to be fulfilled by IBM InfoSphere Guardium.

Various insights have been gained while working on this project. Information security and security management concepts and principles were analyzed and discussed. Additionally, security management approaches have been investigated in detail, as well as several vendors that offer security management solutions. The most important insight gains regard the functioning of the Swedish Armed Forces and the KSF v3.1 In order to construct the component assurance process, a deep understanding of the KSF v3.1 had to be acquired. Moreover, it was necessary to understand how certain undocumented procedures are being carried out in the Swedish Armed Forces. Moreover, a valuable outcome of this master's thesis project is the translation of the KSF v3.1 from Swedish to English language.

A suggestion to others working in this area would be to put a lot of effort into finding high quality sources regarding the security management approaches. Unfortunately, little high quality literature regarding these security management approaches, especially SIEM, is available.

7.2 Limitations

Several limitations were encountered during this research. The first limitation concerns the security market research, which was performed based on analyzing the Gartner Magic Quadrants market research reports. Although these reports have represented the most influential source of vendor information for many years, it would be desirable if the research could have been conducted directly by the author. However, due to the time duration of this project and the resources that would have been needed for such research, it was impossible to conduct this research myself. Another limitation

was that KSF v3.1 is not written very comprehensibly. Moreover, the comparison between the two leading security management solutions and the assurance requirements stated in the KSF v3.1 was limited because the documentation concerning the IBM InfoSphere Guardium and RSA Archer was not written according to the KSF v3.1 and its assurance requirements. The documentation concerning RSA Archer was particularly undetailed. Unfortunately, it was not possible to acquire more detailed documentation from the vendor because I did not have the authority to request such documentation on behalf of the Swedish Armed Forces. Overall, these limitations did not affect the outcome of this Master's thesis project.

7.3 Future work

All of the goals stated in the beginning of the research were met. However, the research could be expanded by performing market research without using the Gartner Magic Quadrants market research reports. Additionally, as mentioned in Section 6.2.5 when a component cannot meet all the requirements that are needed for that component to be assigned to a certain component assurance level, the developer must explain why the introduction of this component does not jeopardize the security of the organization; hence, this process should be analyzed and documented. The research could also be expanded by comparing the similarities between the KSF v3.1 and the Common Criteria. As previously mentioned, KSF v3.1 is written based on the Common Criteria. Hence, it would be beneficial to compare the KSF v3.1 and an international standard such as the Common Criteria. Furthermore, the IBM InfoSphere Guardium and the Common Criteria could be linked in that manner. In addition, the component assurance process or some parts of it could be automatized.

7.4 Reflections

The most obvious ethical aspect of this work was investigating methods for protecting users and organizations. Selecting the best security management solution assists in providing this protection. The implementation of a security management solution in the Swedish Armed Forces not only improves the security of the organization itself but also the Swedish society. Moreover, the Swedish Armed Forces maintain relationships with many other countries and having an efficient security management solution will improve the security of these relationships. The outcome of this master's thesis project lays the groundwork for an automation process and makes the compliance process more efficient in the future. Hence, the research will help streamline the process to some extent.

References

[1] Swedish Armed Forces, 'KSF Krav på IT-säkerhetsförmågor hos IT-system v3.1'. Swedish Armed Forces, 13-Jun-2016.

[2] Swedish Armed Forces, 'Intelligence and security service', *Försvarsmakten*. [Online]. Available: http://www.forsvarsmakten.se/en/our-organisation/our-forces/intelligence-and-security-service/. [Accessed: 19-May-2016]

[3] 'Gartner Magic Quadrant Enhancements'. [Online]. Available: http://www.gartner.com/technology/research/magic-quadrants/. [Accessed: 19-May-2016]

[4] 'Technology Research | Gartner Inc.' [Online]. Available: http://www.gartner.com/technology/home.jsp. [Accessed: 19-May-2016]

[5] 'About The Common Criteria : New CC Portal'. [Online]. Available: https://www.commoncriteriaportal.org/ccra/. [Accessed: 19-May-2016]

[6] 'SANS Institute: Information Security Resources'. [Online]. Available: https://www.sans.org/information-security/. [Accessed: 19-May-2016]

[7] Clive Vermeulen and Rossouw Von Solms, 'The information security management toolbox – taking the pain out of security management', *Information Management & Computer Security*, vol. 10, no. 3, pp. 119–125, Aug. 2002. DOI: 10.1108/09685220210431872

[8] Richard Kissel, 'Glossary of key information security terms', National Institute of Standards and Technology, NIST IR 7298r2, May 2013 [Online]. Available: http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf. [Accessed: 19-May-2016]

[9] 'Introduction to Information Security | US-CERT'. [Online]. Available: https://www.us-cert.gov/security-publications/introduction-information-security. [Accessed: 19-May-2016]

[10] William Stallings, *Network Security Essentials: Applications and Standards*, Fifth edition. Boston: Pearson, 2014, ISBN: 978-0-13-337043-0.

[11] Darril Gibson, 'Understanding The Security Triad (Confidentiality, Integrity, and Availability) | Understanding the Security Triad (Confidentiality, Integrity, and Availability) | Pearson IT Certification', 27-May-2011. [Online]. Available: http://www.pearsonitcertification.com/articles/article.aspx?p=1708668. [Accessed: 19-May-2016]

[12] 'Hash Functions'. [Online]. Available: http://www.sans.edu/research/security-laboratory/article/hash-functions. [Accessed: 19-May-2016]

[13] 'ISO/IEC 27000:2009 - Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary', *ISO*. [Online]. Available: http://www.iso.org/iso/catalogue_detail?csnumber=41933. [Accessed: 19-May-2016]

[14] R. Shirey, 'Internet Security Glossary'. Internet Request for Comment, vol. RFC 2828 (Informational), May-2000 [Online]. Available: http://www.rfc-editor.org/rfc/rfc2828.txt

[15] William Stallings, *Cryptography and network security: principles and practice*, 5th ed. Boston: Prentice Hall, 2011, ISBN: 978-0-13-609704-4.

[16] Rick Lehtinen, Deborah Russell, G. T. Gangemi, and Deborah Russell, *Computer security basics*, 2nd ed. Sebastopol, CA: O'Reilly & Associates, 2006, ISBN: 978-0-596-00669-3.

[17] *SS-ISO/IEC 17799:2005*, 2nd ed. Stockholm, Sweden: Swedish Standards Institute, 2005.

[18] Bel G. Raggad, *Information security management: concepts and practice*, 1st ed. Boca Raton, FL: CRC Press/Taylor & Francis, 2010, ISBN: 978-1-4200-7854-1.

[19] Catherine Paquet, 'Chapter 1 Network Security Concepts and Policies', in *Implementing Cisco IOS network security (IINS): foundation learning guide*, 2nd ed., Indianapolis, Indiana, USA: Cisco Press, 2013.

[20] 'ISO IEC 27000 2014 Information Security Definitions', 12-Nov-2013. [Online]. Available: http://www.praxiom.com/iso-27000-definitions.htm. [Accessed: 20-May-2016]

[21] Bradley Hart, 'Implementing a Successful Security Assessment Process'. Interested in learning more about security? SANS Institute InfoSec Reading Room, 21-Aug-2001 [Online]. Available: https://www.sans.org/reading-room/whitepapers/basics/implementing-successful-security-assessment-process-450

[22] 'Security Auditing Overview', *Technet.microsoft.com*, 03-Jul-2013. [Online]. Available: https://technet.microsoft.com/en-us/library/dn319078.aspx. [Accessed: 20-May-2016]

[23] Joseph Zadjura, 'An Introduction to Certification and Accreditation'. SANS Institute InfoSec Reading Room, 21-Sep-2003 [Online]. Available: https://www.sans.org/reading-room/whitepapers/accreditation/introduction-certification-accreditation-1259

[24] 'ISO/IEC 27001 - Information security management', *ISO*. [Online]. Available: http://www.iso.org/iso/iso27001. [Accessed: 20-May-2016]

[25] Karen Scarfone and Peter Mell, 'Guide to Intrusion Detection and Prevention Systems (IDPS)'. National Institute of Standards and Technology, Feb-2007 [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf

[26] Shon Harris, *CISSP certification exam guide*. New York: McGraw-Hill/Osborne, 2002, All-in-one, ISBN: 978-0-07-219354-1.

[27] Anargyros Chryssanthou, Ioannis Apostolakis, and Iraklis Varlamis, Eds., *Certification and Security in Health-Related Web Applications: Concepts and Solutions*. IGI Global, 2011, ISBN: 978-1-61692-895-7 [Online]. Available: http://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/978-1-61692-895-7. [Accessed: 23-May-2016]

[28] Ryan Mazerik, 'Information Security Policies - InfoSec Resources'. [Online]. Available: http://resources.infosecinstitute.com/information-security-policies/. [Accessed: 23-May-2016]

[29] Paul Johnson, 'What are Policies, Standards, Guidelines and Procedures? | MindfulSecurity.com – The Information Security Awareness Resource'. [Online]. Available: http://mindfulsecurity.com/2009/02/03/policies-standards-and-guidelines/. [Accessed: 23-May-2016]

[30] 'ISO 27000 - An Introduction to ISO 27001 / ISO27001'. [Online]. Available: http://www.27000.org/iso-27001.htm. [Accessed: 23-May-2016]

[31] Organisation for Economic Co-operation and Development and SourceOECD (Online service), *OECD guidelines for multinational enterprises*. Paris: OECD, 2008, ISBN: 978-92-64-06032-6 [Online]. Available: http://dx.doi.org/10.1787/9789264060326-en. [Accessed: 23-May-2016]

[32] Ariffuddin Aizuddin, 'The Common Criteria ISO/IEC 15408 - The Insight, Some Thoughts, Questions and Issues', 2001 [Online]. Available: https://www.sans.org/reading-room/whitepapers/standards/common-criteria-iso-iec-15408-insight-thoughts-questions-issues-545

[33] James P. McGreevy, 'Footprinting: What Is It, Who Should Do It, and Why?', 2002 [Online]. Available: https://www.sans.org/reading-room/whitepapers/auditing/footprinting-it-it-why-62

[34] Charles P. Pfleeger and Shari Lawrence Pfleeger, *Analyzing Computer Security: A Threat/vulnerability/countermeasure Approach*. Prentice Hall Professional, 2012, ISBN: 978-0-13-278946-2.

[35] 'Computer Virus: What It Is and What It Does'. [Online]. Available: https://www.microsoft.com/en-us/safety/pc-security/virus-whatis.aspx. [Accessed: 23-May-2016]

[36] Jon Maurer, 'Internet Worms: Walking on Unstable Ground'. SANS Institute InfoSec Reading Room, 2003 [Online]. Available: https://www.sans.org/reading-room/whitepapers/malicious/internet-worms-walking-unstable-ground-1229

[37] 'Computer Worm', *Veracode*, 02-Feb-2014. [Online]. Available: http://www.veracode.com/security/computer-worm. [Accessed: 23-May-2016]

[38] Victor Velasco, 'Introduction to IP Spoofing'. SANS Institute InfoSec Reading Room, 21-Nov-2000 [Online]. Available: https://www.sans.org/reading-room/whitepapers/threats/introduction-ip-spoofing-959

[39] Stephen Northcutt, 'Denial of Service', *SANS Technology Institute*. [Online]. Available: http://www.sans.edu/research/security-laboratory/article/denial-of-service. [Accessed: 23-May-2016]

[40] Gary C. Kessler, 'Defenses Against Distributed Denial of Service Attacks'. SANS Institute InfoSec Reading Room [Online]. Available: https://www.giac.org/paper/gsec/236/defenses-distributed-denial-service-attacks/100755

[41] Stuart McDonald, 'SQL Injection: Modes of Attack, Defence, and Why It Matters'. SANS Institute InfoSec Reading Room, 08-Apr-2002 [Online]. Available: https://www.sans.org/reading-room/whitepapers/securecode/sql-injection-modes-attack-defence-matters-23

[42] 'Understanding SQL Injection', *Cisco*. [Online]. Available: http://www.cisco.com/c/en/us/about/security-center/sql-injection.html. [Accessed: 23-May-2016]

[43] Roger Grimes, 'Types of Password Attacks', 30-Jan-2006. [Online]. Available: http://windowsitpro.com/security/types-password-attacks. [Accessed: 23-May-2016]

[44] Brad Ruppert, 'Protecting Against Insider Attacks'. SANS Institute InfoSec Reading Room, 02-Apr-2009 [Online]. Available: https://www.sans.org/reading-room/whitepapers/incident/protecting-insider-attacks-33168

[45] Harold F Tipton and Micki Krause, 'Chapter 9: Security Information and Event Management (SIEM) Technology', in *Information Security Management Handbook, Sixth Edition, 3*, 6th ed., vol. 3rd, Hoboken: CRC Press, 2009, pp. 112–125 [Online]. Available: http://www.SLQ.eblib.com.au/patron/FullRecord.aspx?p=570476. [Accessed: 23-May-2016]

[46] Hervé Debar and Jouni Viinikka, 'Security information management as an outsourced service', *Information Management & Computer Security*, vol. 14, no. 5, pp. 417–435, Oct. 2006. DOI: 10.1108/09685220610707430

[47] Stuart Jacobs, 'Chapter 5: OPERATIONAL MANAGEMENT OF SECURITY', in *Security management of next generation telecommunications networks and services*, John Wiley & Sons, 2014, pp. 277–317 [Online]. Available: http://www.books24x7.com/marc.asp?bookid=63715. [Accessed: 23-May-2016]

[48] John R. Vacca, *Computer and Information Security Handbook*. Newnes, 2012, ISBN: 978-0-12-394612-6.

[49] Adam Gordon and Steven Hernandez, *The Official (ISC)2 Guide to the SSCP CBK*. John Wiley & Sons, 2016, ISBN: 978-1-119-27863-4.

[50] Mark Nicolett and Kelly M. Kavanagh, 'Critical Capabilities for Security Information and Event Management'. Gartner, Inc., 07-May-2013 [Online].

Available: http://dss.lv/f/Critical_Capabilities_for_Security_Information_and_Event_Management_-_2013_Q1Labs_IBM_Security_Systems.pdf

[51] David R. Miller, Shon Harris, Allen Harper, Stephen VanDyke, and Chris Blask, *Security Information and Event Management (SIEM) Implementation*, 1st ed. New York: McGraw-Hill Education, 2010, ISBN: 978-0-07-170109-9.

[52] R. Gerhards, 'RFC 5424 - The Syslog Protocol'. Mar-2009 [Online]. Available: https://tools.ietf.org/pdf/rfc5424.pdf

[53] Amrit T. Williams and Mark Nicolett, 'Improve IT Security With Vulnerability Management', 02-May-2005. [Online]. Available: https://www.gartner.com/doc/480703/improve-it-security-vulnerability-management. [Accessed: 24-May-2016]

[54] 'IDFAQ: What is a Host Intrusion Detection System?', *SANS - Information Security Resources*. [Online]. Available: https://www.sans.org/security-resources/idfaq/what-is-a-host-intrusion-detection-system/1/24. [Accessed: 24-May-2016]

[55] Jonathan Chee, 'Host Intrusion Prevention Systems and Beyond'. SANS Institute InfoSec Reading Room, 02-Jun-2008 [Online]. Available: https://www.sans.org/reading-room/whitepapers/intrusion/host-intrusion-prevention-systems-32824

[56] Phalguni Gupta, Surya Prakash, and Umarani Jayaraman, *IT Infrastructure and Its Management*. Tata McGraw-Hill Education, 2010, ISBN: 978-0-07-068184-2.

[57] 'Configuration items', *IBM Knowledge Center*, 01-Jan-2013. [Online]. Available: http://www.ibm.com/support/knowledgecenter/SSZRHJ/com.ibm.sccd-saas.doc/config/c_config_item.html. [Accessed: 24-May-2016]

[58] Stephen Northcutt, 'IDFAQ: What is network based Intrusion Detection?', *SANS - Information Security Resources*. [Online]. Available: https://www.sans.org/security-resources/idfaq/what-is-network-based-intrusion-detection/2/3. [Accessed: 24-May-2016]

[59] Thomas M. Thomas and Donald Stoddard, 'Chapter 11: Intrusion Detection and Honeypots', in *Network Security First-Step*, Cisco Press, 2011.

[60] 'Network Monitoring', in *Mac® Security Bible*, Indianapolis, IN, USA: Wiley Publishing, Inc., 2011, pp. 665–690 [Online]. Available: http://doi.wiley.com/10.1002/9781118257739.ch22. [Accessed: 24-May-2016]

[61] 'Governance, Risk, and Compliance'. KPMG, 2008 [Online]. Available: https://www.kpmg.com/US/en/IssuesAndInsights/ArticlesPublications/Documents/governance-risk-compliance.pdf

[62] Russ Banham, 'Is ERM GRC? Or Vice Versa?', *Treasury & Risk magazine*, Jun-2007 [Online]. Available: http://www.treasuryandrisk.com/2007/06/01/is-erm-grc-or-vice-versa-". [Accessed: 25-May-2016]

[63] Carol S. Switzer, Scott L. Mitchell, and Jason Lee Mefford, 'GRC Capability Model'. OCEG, Dec-2015 [Online]. Available: http://www.oceg.org/resources/red-book-3/

[64] Paul Proctor, 'Why I Hate the Term GRC', *Gartner Blog Network*. 13-May-2013 [Online]. Available: http://blogs.gartner.com/paul-proctor/2013/05/13/why-i-hate-the-term-grc/. [Accessed: 25-May-2016]

[65] 'The Role of Governance, Risk Management & Compliance in Organizations'. Ponemon Institute, May-2011 [Online]. Available: http://www.emc.com/collateral/about/news/ponemon-report-egrc.pdf

[66] John A. Wheeler, 'Gartner Launches Integrated GRC Research Program', *Gartner Blog Network*. 08-Jun-2015 [Online]. Available: http://blogs.gartner.com/john-wheeler/gartner-launches-integrated-grc-research-program/. [Accessed: 25-May-2016]

[67] Basel Committee on Banking Supervision, Ed., *Principles for the sound management of operational risk*, June 2011. Basel: Bank for International Settlements, 2011, ISBN: 978-92-9197-857-1.
[68] Mark Bevir, *Governance: A Very Short Introduction*. OUP Oxford, 2012, ISBN: 978-0-19-164629-4.
[69] 'Concept of governance', *Education | United Nations Educational, Scientific and Cultural Organization*. [Online]. Available: http://www.unesco.org/new/en/education/themes/strengthening-education-systems/quality-framework/technical-notes/concept-of-governance/. [Accessed: 26-May-2016]
[70] 'IT Governance (ITG)', *Gartner IT Glossary*, 08-Feb-2012. [Online]. Available: http://www.gartner.com/it-glossary/it-governance/. [Accessed: 26-May-2016]
[71] Anthony Tarantino, *The Governance, Risk, and Compliance Handbook: Technology, Finance, Environmental, and International Guidance and Best Practices*, 1st ed. Hoboken, N.J: Wiley, 2008, ISBN: 978-0-470-09589-8.
[72] 'ISO/IEC 38500:2015(en), Information technology — Governance of IT for the organization', *ISO*. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:38500:ed-2:v1:en. [Accessed: 26-May-2016]
[73] 'ITIL', *AXELOS*. [Online]. Available: https://www.axelos.com/best-practice-solutions/itil. [Accessed: 26-May-2016]
[74] 'COBIT - IT Governance Framework - Information Assurance Control | ISACA', *ISACA*. [Online]. Available: http://www.isaca.org/Knowledge-Center/cobit/Pages/Overview.aspx. [Accessed: 28-May-2016]
[75] 'ISO/IEC 27002:2013(en), Information technology — Security techniques — Code of practice for information security controls', *ISO*. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en. [Accessed: 28-May-2016]
[76] 'ISO 31000:2009(en), Risk management — Principles and guidelines', *ISO*. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en. [Accessed: 29-May-2016]
[77] Tobias Ackermann, *IT Security Risk Management: Perceived IT Security Risks in the Context of Cloud Computing*. Springer Science & Business Media, 2012, ISBN: 978-3-658-01115-4.
[78] 'ISO 19600:2014(en), Compliance management systems — Guidelines', *ISO*. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso:19600:ed-1:v1:en. [Accessed: 30-May-2016]
[79] 'The IBM Risk and Compliance Framework: addressing the challenges of compliance'. IBM, Jan-2005 [Online]. Available: http://www-07.ibm.com/hk/infrastructuresolutions/downloads/rcf-white-paper-01-25-05.pdf
[80] 'PCI DSS Quick Reference Guide'. PCI Security Standards Council, Oct-2010 [Online]. Available: https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf
[81] 'The Sarbanes-Oxley Act 2002', 2006. [Online]. Available: http://www.soxlaw.com/. [Accessed: 31-May-2016]
[82] 'IT Compliance Management Guide'. Microsoft Corporation, Oct-2008.
[83] 'Identity Management - Access Management - Gartner Research', *Gartner IT Glossary*, 08-Feb-2012. [Online]. Available: http://www.gartner.com/it-glossary/identity-and-access-management-iam/. [Accessed: 01-Jun-2016]
[84] Ertem Osmanoglu, *Identity and Access Management: Business Performance Through Connected Intelligence*, 1 edition. Amsterdam, Netherlands: Syngress, 2013, ISBN: 978-0-12-408140-6.

[85] 'Identity and Access Management', in *IT Audit, Control, and Security*, Hoboken, NJ, USA: John Wiley & Sons, Inc., 2012, pp. 472–485 [Online]. Available: http://doi.wiley.com/10.1002/9781118269138.ch22. [Accessed: 02-Jun-2016]

[86] 'Authentication', in *Information Security*, Hoboken, NJ, USA: John Wiley & Sons, Inc., 2011, pp. 227–264 [Online]. Available: http://doi.wiley.com/10.1002/9781118027974.ch7. [Accessed: 02-Jun-2016]

[87] Robert J. Bartz, *Mobile Computing Deployment and Management: Real World Skills for CompTIA Mobility+ Certification and Beyond*. John Wiley & Sons, 2015, ISBN: 978-1-118-82464-1.

[88] Butler W. Lampson, 'Protection', *SIGOPS Operating Systems Review*, vol. 8, no. 1, pp. 18–24, Jan. 1974. DOI: 10.1145/775265.775268

[89] David Black and Julie Thomas, 'How Markets and Vendors Are Evaluated in Gartner Magic Quadrants', 22-Jul-2014. [Online]. Available: https://www.gartner.com/doc/2804921/markets-vendors-evaluated-gartner-magic. [Accessed: 04-Jun-2016]

[90] Kelly M. Kavanagh and Oliver Rochford, 'Magic Quadrant for Security Information and Event Management', Gartner, Inc., G00267505, Jul. 2015 [Online]. Available: https://www.gartner.com/doc/reprints?id=1-2JM4RVZ&ct=150720&st=sb

[91] Paul E. Proctor and John A. Wheeler, 'Magic Quadrant for IT Risk Management', Gartner, Inc., G00261240, Mar. 2015 [Online]. Available: https://www.gartner.com/doc/3003517/magic-quadrant-it-risk-management

[92] John A. Wheeler and Jie Zhang, 'Magic Quadrant for Operational Risk Management Solutions', Gartner, Inc., G00273347, Dec. 2015 [Online]. Available: https://www.gartner.com/doc/3177919/magic-quadrant-operational-risk-management

[93] Christopher Ambrose, Gayla Sullivan, and Kris Doering, 'Magic Quadrant for IT Vendor Risk Management', Gartner, Inc., G00263243, Oct. 2014 [Online]. Available: https://www.gartner.com/doc/2890717/magic-quadrant-it-vendor-risk

[94] Felix Gaehtgens and Brian Iverson, 'Definition: Identity Governance and Administration', Gartner, Inc., Definition: Identity Governance and Administration, Jul. 2015.

[95] Whei-Jen Chen, Boaz Barkai, Joe M. DiPietro, Vladislav Langman, Daniel Perlov, Roy Riah, Yosef Rozenblit, Abdiel Santos, and I. B. M. Redbooks, *Deployment Guide for InfoSphere Guardium*. IBM Redbooks, 2015, ISBN: 978-0-7384-3935-8.

[96] 'IBM Data security and protection', 05-Jun-2016. [Online]. Available: http://www-03.ibm.com/software/products/en/category/data-security. [Accessed: 07-Jun-2016]

[97] 'IBM Security Guardium Data Activity Monitor'. [Online]. Available: http://www-03.ibm.com/software/products/en/ibm-security-guardium-data-activity-monitor. [Accessed: 07-Jun-2016]

[98] 'IBM Security Guardium for Files'. [Online]. Available: http://www-03.ibm.com/software/products/en/ibm-security-guardium-for-files. [Accessed: 08-Jun-2016]

[99] 'IBM Security Guardium Data Redaction'. [Online]. Available: http://www-03.ibm.com/software/products/en/ibm-security-guardium-data-redaction. [Accessed: 08-Jun-2016]

[100] 'IBM Security Guardium Vulnerability Assessment', 01-Jan-2016. [Online]. Available: http://www-03.ibm.com/software/products/en/security-guardium-vulnerability-assessment. [Accessed: 08-Jun-2016]

[101] 'IBM Security Guardium Express Activity Monitor for Databases', 01-Jan-2016. [Online]. Available: http://www-03.ibm.com/software/products/en/ibm-security-guardium-express-activity-monitor-for-databases. [Accessed: 08-Jun-2016]

[102] ‘IBM Security Guardium Data Encryption’. [Online]. Available: http://www-03.ibm.com/software/products/en/ibm-security-guardium-data-encryption. [Accessed: 08-Jun-2016]
[103] ‘RSA Archer: IT and Security Risk Management’. [Online]. Available: https://www.rsa.com/en-us/products-services/governance-risk-compliance/it-and-security-risk-management. [Accessed: 08-Jun-2016]
[104] ‘RSA Archer: Enterprise & Operational Risk Management’. [Online]. Available: https://www.rsa.com/en-us/products-services/governance-risk-compliance/enterprise-operational-risk-management. [Accessed: 08-Jun-2016]
[105] ‘RSA Archer: Regulatory and Corporate Compliance Management’. [Online]. Available: https://www.rsa.com/en-us/products-services/governance-risk-compliance/regulatory-and-corporate-compliance-management. [Accessed: 08-Jun-2016]
[106] ‘RSA Archer: Audit Management’. [Online]. Available: https://www.rsa.com/en-us/products-services/governance-risk-compliance/audit-management. [Accessed: 08-Jun-2016]
[107] ‘RSA Archer: Business Resiliency’. [Online]. Available: https://www.rsa.com/en-us/products-services/governance-risk-compliance/business-resiliency. [Accessed: 11-Jun-2016]
[108] ‘RSA Archer: GRC Platform’. [Online]. Available: https://www.rsa.com/en-us/products-services/governance-risk-compliance/grc-platform. [Accessed: 11-Jun-2016]
[109] ‘Säkerhetsskyddsförordning (1996:633)’ [Online]. Available: http://www.notisum.se/rnp/sls/lag/19960633.HTM. [Accessed: 26-Jun-2016]
[110] United States Air Force, ‘Military Standard: Technical Reviews and Audits for Systems, Equipments, and Computer Software’, United Stated Department of Defense, Washington, D.C. 20301, Military Standard MIL-STD-1521B, Jun. 1985 [Online]. Available: http://www.dtic.mil/dtic/tr/fulltext/u2/a285777.pdf

Appendix A: KSF v3.1: Requirements for IT security capabilities of IT systems

KSF

Requirements for IT security capabilities of IT systems

v3.1

TABLE OF CONTENTS

1 Introduction

1.1 Opening

KSF[1] are the requirements on IT security capabilities that Military Intelligence and Security Service (MUST) has produced and which, under C MUST decisions[2], all the IT systems[3] in the Armed Forces must meet in order for the adequate protection to exist. In this perspective, KSF is a part of MUST risk management regarding IT security capabilities to reduce or eliminate the estimated risks in terms of IT systems.

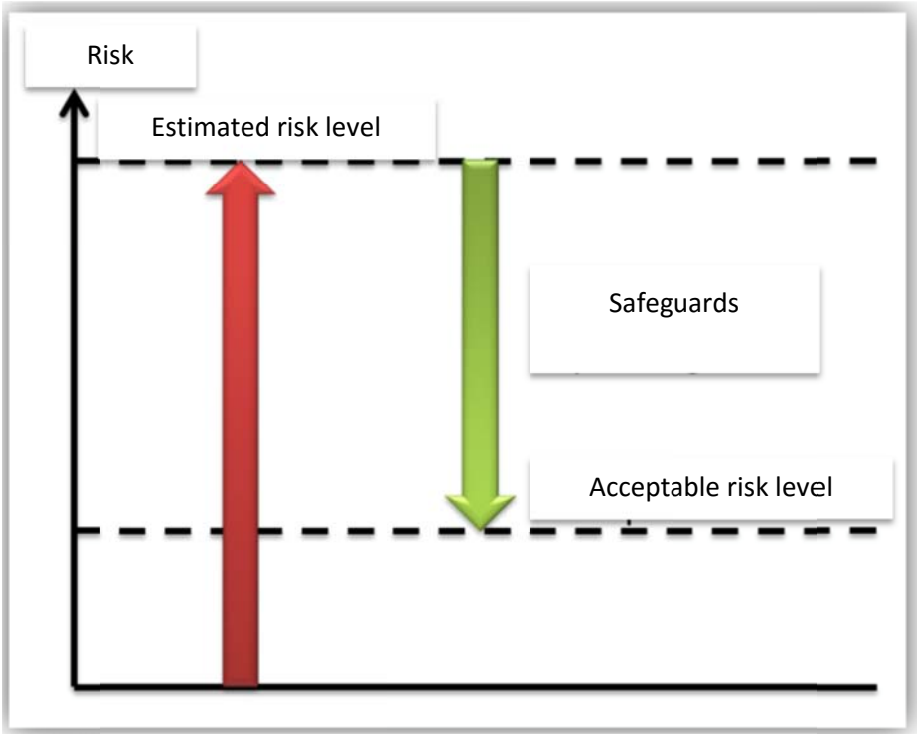

Figure 1 Relationship between assessed risks and protective measures in KSF

For better readability in this document, the prefix IT has been removed from the words “IT security capabilities" and "IT systems", but the meaning remains the same. In the case of a different meaning, it is indicated separately.

[1] Requirements for safety features
[2] KSF version 2.0 - Decision on requirements for certified safety functions, verse. 2.0, HQ Comm. 2004- 12-20 bet. 10 750: 78 976
[3] With IT systems referred to under Chapter 7. 1 § 2 The Armed Forces Regulations (FFS 2003: 7) on security systems with technology that manages and exchanges information with the surroundings.

1.2 Objectives, targets

KSF is primarily used when defining IT security requirements that give the system its security capabilities before purchasing and when MUST evaluates IT system from the safety view before MUST opinion for accreditation. These requirements are a part of the Armed Forces requirements definition for IT systems within the IT process.

In terms of a system's life cycle, KSF focuses on setting requirements for development of the system, i.e. the process leading to accreditation. This is because IT security and confidence in the system's security capability needs to be built into the system from the start and not added as final action on already developed system.

KSF is aimed primarily at personnel in the Armed Forces and external organizations that set the requirements and acquire IT systems for the Armed Forces account.

KSF does not address directly those who develop IT systems, when they instead are the recipients of the complete specification of requirements on the IT system, which originates in the KSF.

If the system has adequate security abilities does not guarantee that the system is used in a safe manner because the responsibility for this ultimately is the responsibility of the user. Monitoring of safe use is done through the control activities carried out within the framework of the respective responsibility roles under the life-cycle model and the Armed Forces Chief Information Officer (CIO). In addition, it carries out the military security service security control, where IT security is a subset.

1.3 Roles

KSF is produced by CIO IT Management model[4], which means that the following terms are used:

- **Buyers** are the ones that decide, order and finance an IT service[5]. The buyer is responsible for the operation or area expertise according FM ArbO.
- **Coordinator** is responsible for preparing and coordinating the requirements definition for IT services. Coordinator is also responsible for directing, ordering and follow up of the production of IT services. Responsibility for the subject matter of IS/IT and information infrastructure is also coordinators.

---

[4] HKV 2011-10-31 09100:64970
[5] The cost of the IT infrastructure is financed (cost allocated) also by clients

- **Executors**[6] are those that produce and provide IT services. Another way to put it is that they are suppliers.
- **Occupants**, finally, are those who use IT services in the business.

1.4 The relation to operational-, constitutional- and safety analysis

Figure 2 describes on a general level the connection between operational, constitutional and safety analysis and KSF. This is described briefly below.

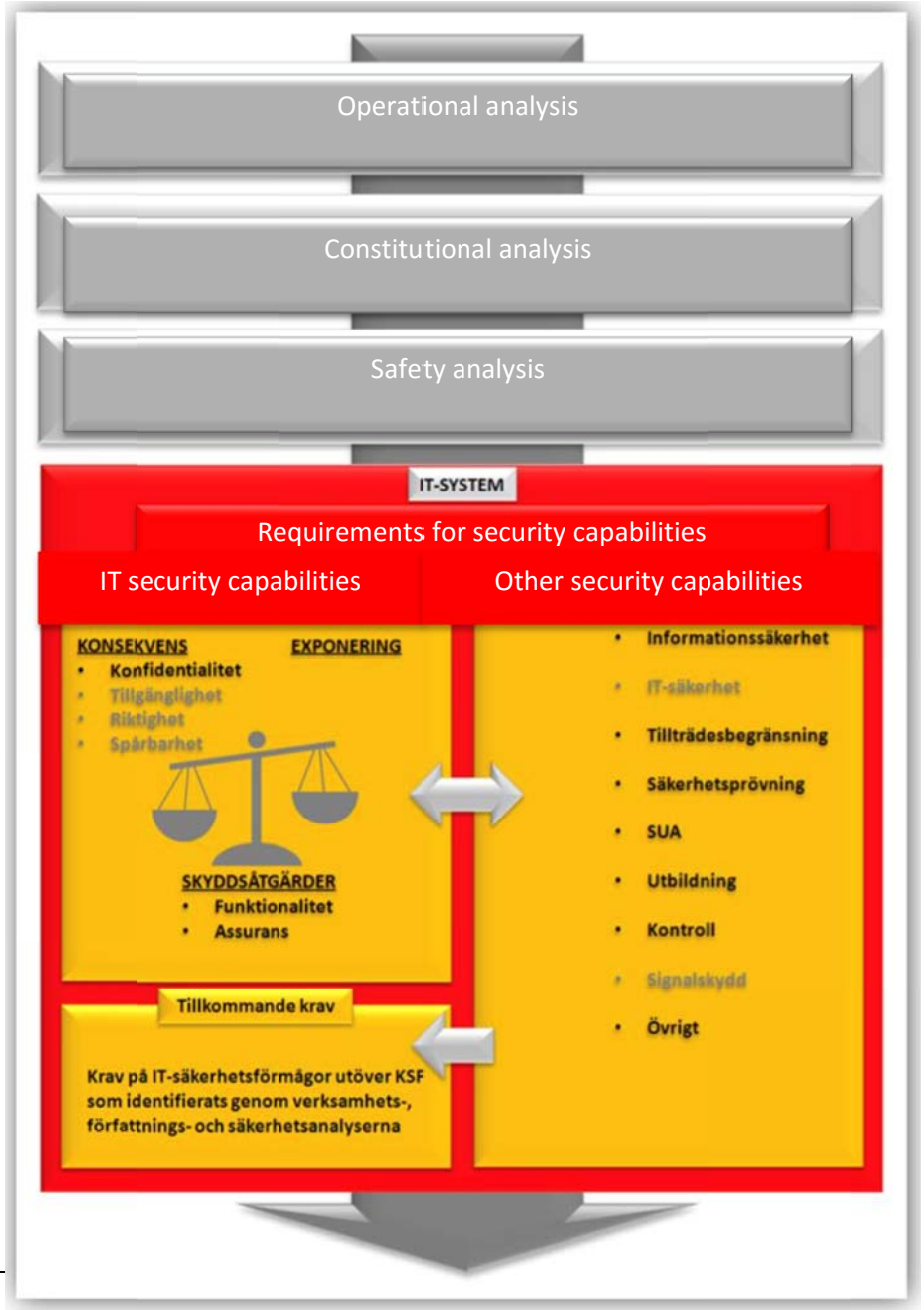

Figure 2 Correlation between operational, constitutional and safety analysis and KSF

[6] Internal organizational unit within the Armed Forces that delivers all or part of the IT service called internal providers, such are FMLOG or FMTM. Other agencies, companies and organizations via contracts deliver the whole or parts of the IT service are called external providers, such as the FMV or industry (HQ 2011-04-08 09 100: 56 741).

1.4.1 *Operational analysis*

An operational analysis describes in one security context, the activities of an IT system is intended to support, the types of data that the IT system is intended to treat (e.g., privacy assessment) as well as the operational requirements of protection (e.g. in the case availability). An operational analysis provides a basis for constitutional analysis and safety analysis.

1.4.2 *Constitutional analysis*

A constitutional analysis is to describe the laws, regulations and internal rules that apply to an IT system and the information referred processed in the IT system.

1.4.3 *Security analysis*

In the safety analysis all worthy of protection resources (personnel, equipment, information, activities and facilities) are identified and prioritized, which will be processed, stored, or otherwise handled by the system (including the system itself) and then made an assessment of the impact occurring and the extent of this data regarding the identified assets exposed to any adverse event affecting the confidentiality, availability, accuracy and traceability.

The result of the safety analysis forms the input values to the KSF by consistency level has been described and assessed according to a set scale. The safety analysis also results in input values to other security requirements. The other security requirements may in some cases constitute input values to the KSF security model, e.g. by affecting the system's exposure. The other safety requirements may also, in some cases, when they are met, provide the operating environment, characteristics that help to meet the KSF. The double arrow in Figure 2 represents this.

1.4.4 *Requirements for IT security capabilities (KSF)*

Through KSF it is assigned which security capabilities a system should at least have what MUST considers to be an acceptable risk level for system in operation in the Armed Forces. As the risk may vary between different systems including the nature, operating environment, the nature and the type of information managed security capabilities need to be adapted to these circumstances. In the KSF an adjustment is made with help of a model and its methodology to identify and describe the requirements. It is to this model business-, constitutional- and security analysis provides input, in terms of consequences and exposure, to allow adjustment and to determine the requirement of the systems IT security capability[7].

---

[7] In Figure 2 above, the input values, availability and traceability gray marked as these in the KSF are not included in the model and thus not managed by specific requirements in the KSF.

1.4.5 Additional requirements

KSF requirements imposed on system's security only one of the armed forces common minimum levels. It is therefore possible for a particular system, safety requirements to be applicable as a result of specific needs (such as high availability), from the laws and regulations (e.g. PUL[8]), or from the activities using the system. These additional safety requirements are identified by the operational and safety analyzes.

1.5 The disposition of the KSF

KSF has the following outline:

- Decision Letter
- Appendix 1 includes the following:
  - Chapter 1 (this chapter) is an introductory description to give the reader an overview of the KSF and can be read as a summary and introduction to the KSF model.
  - Chapter 2 describes the basic principles and the security model that is used to identify the current safety requirements. Chapter 2 lays the foundation for a deeper understanding of the model.
  - Chapter 3 describes the functional safety requirements that define which security capabilities, a system must have.
  - Chapter 4 describes how to identify assurance demands on the system and what level of approval is required by the IT security components.
- Annex 1 contains glossary of terms and acronyms.
- Appendix 2 defines the content of the IT system security specification (ITSS) is. ITSS will describe the system and the safety requirements that the system must meet and how this is done.
- Appendix 3 defines the functional safety requirements that are divided into classes, requirements and requirement components. Requirement components are connected to each requirement level.
- Appendix 4 defines the assurance requirements that are divided into classes, requirements and requirement components. Requirement components are connected to each requirement level.

---

[8] Personal Data Act (1998: 204)

1.6 Constitutional grounds for KSF

This section describes which constitutional support exists for the KSF and there is no constitutional analysis of individual systems. KSF is therefore no compilation of current statutory requirements for systems.

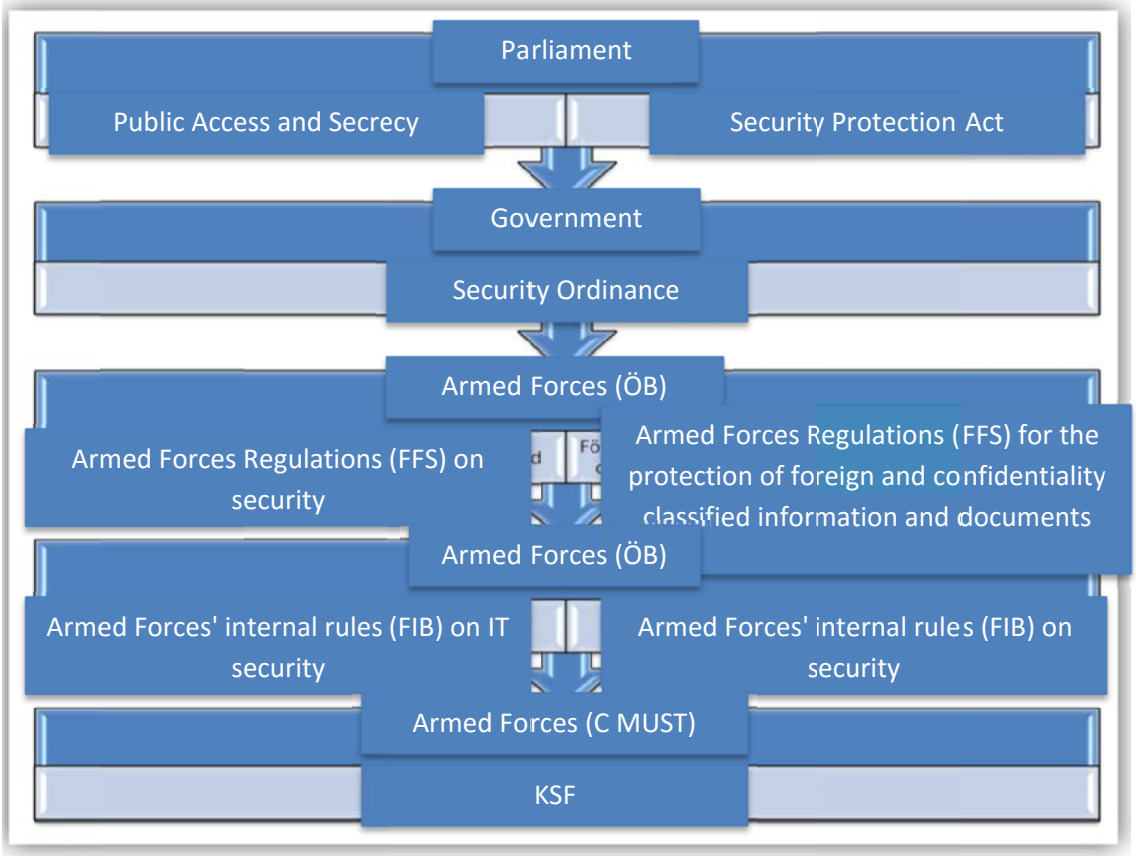

Figure 3 Constitutional grounds for KSF

Security Act (1996:627) and Security Ordinance (1996:633) contain provisions related to security. Details related to the enforcement of these regulations can be found in the Armed Forces Regulations (FFS 2003: 7) on security and the Armed Forces' internal rules (FIB 2007: 2) on security and protection of some equipment. The Armed Forces also decided Armed Forces' internal rules (FIB 2006: 2) on IT security[9]. Both the Security Ordinance that the Armed Forces regulate on security and

[9] The latter constitution was amended by FIB 2010: 2 (also for printing)

the Armed Forces' internal rules on IT security requires approved safety features[10]. Armed Forces Regulations (FFS 2010: 1) on the protection of foreign and confidentiality classified information and documents as well as the Armed Forces' internal rules on IT security also contains provisions on IT security for systems that are also intended for the treatment of foreign classified[11] and confidential classified information as well as information that is not subject to secrecy under the Official Secrets Act (2009: 400), hereafter referred to OSL.

1.6.1 Regarding secret information

Armed Forces' internal rules on IT security show that any system that is intended for the treatment of confidential information shall be provided with approved security functions by MUST.

1.6.2 Regarding foreign classified information

Armed Forces regulations on the protection of foreign and confidentiality classified information and documents[12] state that the foreign classified information shall have the same security features that apply to systems that deal with secret information.

1.6.3 Regarding other information

Armed Forces internal rules on IT security show that any system that is not intended for the treatment of confidential information shall be provided by MUST with approved security features of the system that is intended to be used by several people.

1.7 Model and method

The purpose of the model for the KSF is to unambiguously define the requirements for the safety abilities that a particular system must have and the assurance requirements that provide confidence that the security capabilities exist and that the intended safeguard measures are achieved.

For adaptation of the safety requirements, two factors are considered:

1. The impact of an adverse event that affects privacy (information loss[13]) for the information

[10] Approved security functions specified for access control, security, logging, intrusion detection, protection against compromising signals, protection against unauthorized listening, intrusion prevention and malware protection.
[11] A task of a foreign government or international organization or by a Swedish authority has classified in any of the levels TOP SECRET, SECRET, CONFIDENTIAL or RESTRICTED or equivalent, which is confidential under Chapter 15. 1 § Official Secrets Act but which are not related to national security (1 Chap. 3 § 2 Armed Forces Regulations (FFS 2010: 1) on the protection of foreign and confidentiality classified information and documents).
[12] FFS 2010: 1 Chapter 2. § 1
[13] The KSF is protective only linked to the confidentiality of the information. Possible safeguards for accuracy and accessibility are met to the extent that the requirements of the protection of privacy also can meet these needs. This means that the model for the KSF does not specifically take into account

being processed, stored, or otherwise handled by the system as well.

2. How exposed the system is for actors who can influence the system.

In cases where different judgments will conflict with each other numbness occurs through dialogue with MUST. Examples of this might be where the business availability requirements conflict with the requirement of confidentiality.

1.7.1 *Functional safety requirements*

The functional safety requirements define the security abilities that a system, at least should exhibit. The requirements are divided into different classes[14] where the strength of the requirements represented by the requirement levels Ground (G), Extended (U) or High (H). Functional safety should always be met but this can be done in different ways. The requirements can be met through technical measures in the system, by utilizing properties in its operational environment[15] or by a combination of these (illustrated in Figure 4).

It is the system developer's responsibility to demonstrate for the current IT system that both ATT regulatory compliance exists as well as HUR regulatory compliance are obtained for the functional requirements.

---

the requirements and availability. This does not mean the business analysis identifies those requirements and that these requirements are quality assured by ITSS documented and evaluated together with the KSF safety.

[14] Corresponds to the approved security functions specified in the FFS and FIB, i.e. access control, security, logging, intrusion prevention, intrusion detection, malware protection, protection against unauthorized interception and protection against compromising signals.

[15] May be, for example, geographical, fortification, personal or administrative nature

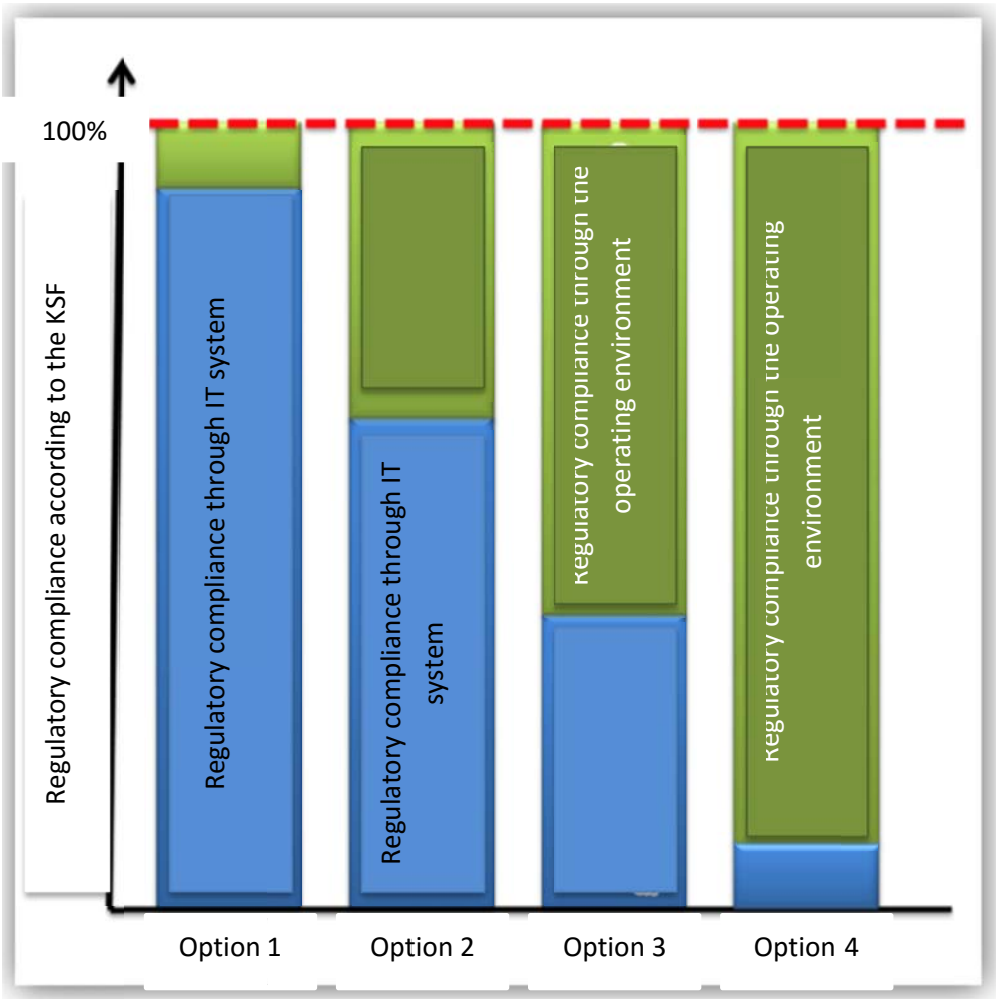

Figure 4 Illustrative examples of alternative ways to achieve regulatory compliance

1.7.2 Assurance requirements

Assurance requirements specify how confidence in the security capabilities will be demonstrated. Assurance requirements are divided into different classes where the strength of the requirements is represented by the requirement levels Ground (G), Extended (U) or High (H) in the same way as the functional safety requirements.

Assurance[16] will also appear for the properties in its operational environment. With regulatory compliance through the application-operating environment referred to in these cases are not

[16] Confidence and trust to the property gives the intended effect.

possibilities to reduce the system's exposure but rather the characteristics of the application-operating environment wholly or partially contribute to the fulfillment of certain security capabilities.

It is the system developer's responsibility to demonstrate for the current IT system that both ATT regulatory compliance exists as well as HUR regulatory compliance are obtained for the assurance requirements.

1.7.3 *Evaluation and evaluation methodology*

An evaluation methodology describes how the examination of the system will be implemented, i.e. a procedure to verify that the safety skills and safety requirements are properly identified and that the system meets them. Evaluation methodology also describes how the evaluation should be documented. The purpose of the evaluation methodology is to ensure that evaluation is carried out and documented in a uniform manner and with sufficient quality.

Evaluation methodology is developed independent of the functional and assurance requirements, and addresses only the personnel who will evaluate that a system meets the KSF and to those who will verify that the evaluations are fully and properly implemented.

2 Security model for the KSF

2.1 Introduction

KSF security model is built up on the adaptation of the security capability (through afflicted requirement level) outgoing from the impact assessment of the loss of information in the system and the system's intended exposure. By identifying the extent to which a system can be exposed to attack or abuse, demands on security abilities can be tailored to the assessed risks in the current operating environment. The security model derived for the requirements of security capabilities can be met through technical measures in the system, by utilizing properties in its operational environment[17], or a combination of these.

KSF describes, through assurance requirements, the necessary documentation to demonstrate that the safety functionality of the system is implemented sufficiently and effectively, and to assess and describe the remaining risk.

2.2 KSF security model - the model structure

The both categories, assurance requirements and functional requirements, are in a model structured in a similar way.

Confidence in the system's security features is correct and efficient under the proposed conditions titled assurance, and requires that:

- There is confidence in the origin of the system and its components (when it is very difficult to protect themselves against an unreliable or malicious software developer).
- The processes applied in the development environment for delivery to the operating and management are documented and reliable (as it is very hard to control everything on delivery).
- A system is constructed in a structured way, and that this is documented (otherwise it is not possible to assess the system).
- A system is tested from a relevant safety point of view (to ensure that it exhibits the demands made on IT security capabilities).

[17] May be, for example, geographical, fortification, personal or administrative nature

- User and operation and management organizations get instructions on how the system should be installed, operated and maintained in a safe manner (because the system, in general, would not be used in a planned way and might therefore not be a safe way).
- A system has been analyzed and weaknesses or abnormalities and their consequences documented (to provide a basis for the decision on the system's operational benefits outweigh the risks it entails).

The requirements in the category of functional safety requirements are contained in the annex 3 and the requirements in the category assurance requirements can be found in the Annex 4 of this document.

2.2.1 Requirements structure

The requirements of the KSF are divided into classes that represent a grouping of similar requirements. Each class has a name of four letters beginning with "SF" for functional safety requirements or "SA" for assurance requirements.

Some examples of the assurance identification are the following:

- SFIS - The class of functional safety requirements related to intrusion
- SADE - The class of assurance requirements concerning the IT system architecture and design

Within each class, there are a number of requirements that describe what must be fulfilled. Each requirement has a unique name, as illustrated below:

- SFIS_HRD - A single functional safety requirements of the class of SFI
- SADE_ARK - A single assurance requirements of the class of SADE

For each requirement there are a number of requirement components that show how the requirement can be met. These serial numbers are given according to the following example:

- SFIS_HRD.2 - Other component requirements from the requirement SFIS_ HRD
- SADE_ARK.D1 - The first component requirement from the requirement SADE_ARK

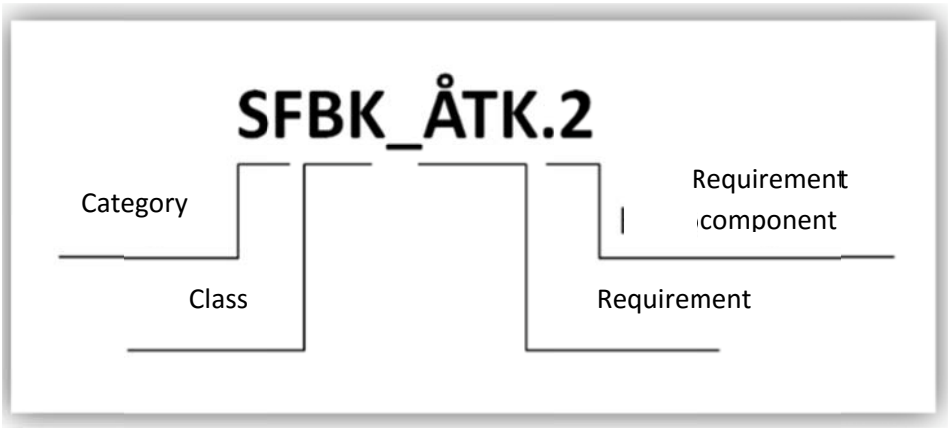

Figure 5 Example of requirements identification

These requirements identifications are separate references to all classes, requirements and components of the KSF and will be used when referring to the KSF requirements document or recorded in the statements of requirements, etc.

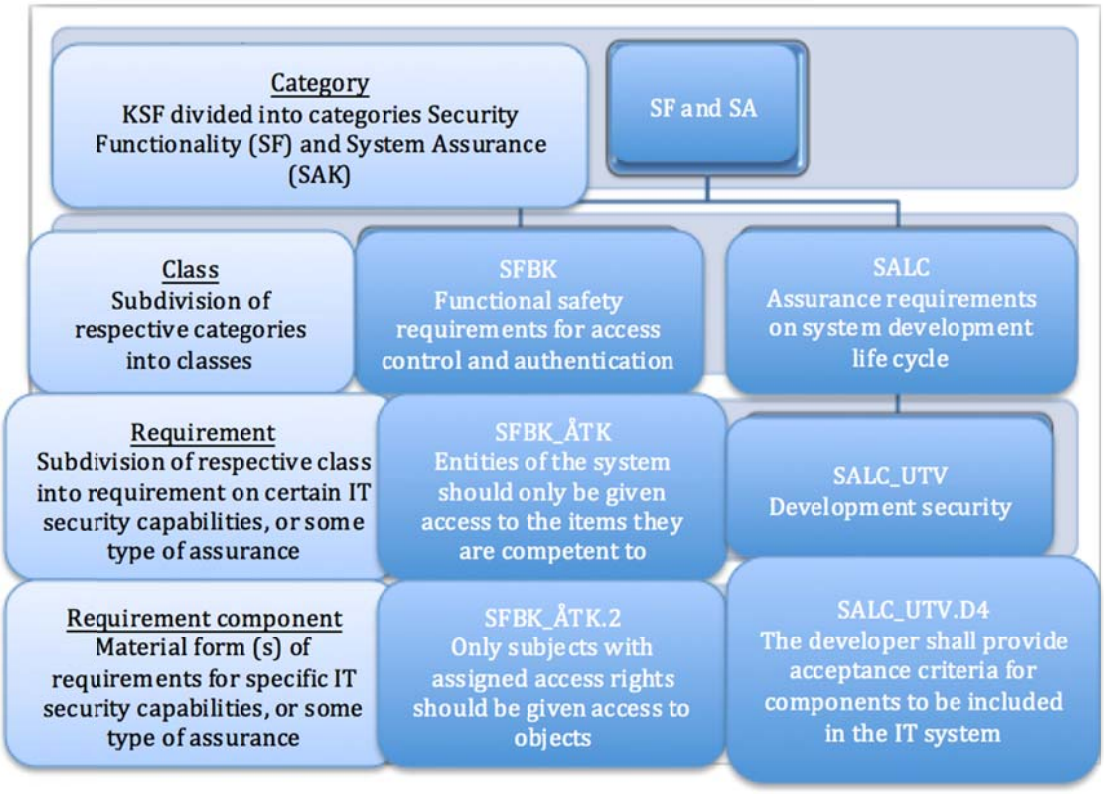

Figure 6: Overall picture of requirements structure and identification

2.3 Safety requirements for systems and components

KSF security model assumes that the system consists of an assembly of components where some components give the system its security capabilities. A system that is composed of certified IT security components can trust that the components are assembled and used as intended. The components are approved by MUST along a grading called component assurance level. Which component assurance level required of the components of a particular system are outlined, though not exhaustive, in Chapter 4. Putting together systems of already approved components could mean a considerable saving of time, instead of every time verifying all incoming IT security components.

2.3.1 Definition of an IT system

In this document the used term IT system is used to name a device that that demands and is assessed according KSF. Such a system may in turn be a "system of systems" but for the sake of the KSF must be applied to each individual part. What level KSF shall apply for the purposes of the Armed Forces IT process through the division into subsystems can however apply KSF smaller units, see 2.3.3.

2.3.2 Dependencies on external components

Some systems rely on security functionality provided by the components not included in the system, e.g. when the system is part of a larger system. In this case, each requirement that has such an external dependency must be clearly identified in IT security specification (ITSS), both its nature and a way in which the requirement is disposed.

External dependencies are only allowed if the external component is part of an accredited system with at least the same level of functional requirements and assurance requirements as the system that relies on the external component. This is to be able to rely on a safety feature in another system. This property must be evaluated and consistent with what the relying system expects from it. The requirement of accreditation also relates to the belief that the external component can protect itself so that the properties are maintained.

2.3.3 Division into subsystems

The breakdown of a system can cost driving requirements isolated to its own subsystems, thereby lowering the total cost of the overall system protection. The possible reduction of the total cost is in this case proportional to the magnitude of the cost driving elements compared with the extent of the non-cost driving elements. The protection for separation between the subsystems shall however always meet the subsystems highest level. Subsystems division provides an opportunity to consider the system as "more collaborative system". From the KSF’s perspective, subsystems are considered as autonomous systems. Each subsystem must meet KSF with regard to functional safety requirements and assurance requirements, and independent ITSS will be compiled for each subsystem.

2.4 Consequence levels

The following describes how the consequence levels are identified for a specific system. The safety analysis identifies the information worth protecting handled by the system. The information was classified under the KSF model for the information classification (according to H SÄK Sekrbed Part A 2011). If the information is KH, H or UK, it should also be assigned to an information security class[18]. This is done through an early mentor and damage assessment (IA). The result determines among other things, information classification system.

Information which after the privacy assessment classified SK are then considered regarding the consistency that arise and the extent of this if the data is disclosed. When the amount of information through the privacy assessment has been classified as SK and then assessed regarding the impact it can also be compared (priority) with H- and UK- data.

The principle of the KSF is to assess the level of impact as a factor in determining the system's level of protection.

To identify the current level of consistency used in KSF, same table (Table 1 below) is a step 1 in the safety analysis[19]. KSF uses the scale from 1 to 5.

Rating		**General impact assessment and impact assessment at the information loss of confidentiality of classified information.**	**Consequence of information loss secret or foreign classified information**[20]
5	Very serious	Expected impact causes an extreme negative effect. The impact involves extremely serious negative effects of large-scale, long-term and constitutes a direct threat to the	Confidential information whose disclosure could cause exceptional harm to Armed Forces or relationship to another state or an international organization or otherwise to national security (top

[18] Investment in information safety occurs through an early "menbedömning" that is the same as an early assessment of the consequence of the information disclosed to unauthorized persons.

[19] H SÄK Skydd 2007

[20] The rate of the disclosure of secret information related to national security is regulated in Chapter 1. 4 § The Armed Forces Regulations on security (FFS 2003: 7), and is described extensively in H SÄK Sekrbed Part A (2011).

		organization. The consequences are not confined to individual abilities or functions within the organization.	secret information). Secret document that has been given the designation TOP SECRET or equivalent from a foreign government or international organization.
4	Serious	Expected impact is significant. The consequences are serious, large-scale or of significance and represents a direct threat, albeit against limited abilities or functions within the organization.	Confidential information whose disclosure could seriously harm the national defense or the relationship to another state or an international organization or otherwise to national security. Secret document has been assigned SECRET or equivalent by a foreign authority or intermediate international organization.
3	Noticeable	Expected consequences are not insignificant and compromises, causing injury, prevent, facilitate, means more interruptions and brings tangible negative effects albeit to a limited extent.	Confidential information whose disclosure could lead to a not insignificant but for the Armed Forces or the relationship to another state or an international organization or otherwise to national security. Secret document which has been given the designation CONFIDENTIAL or the equivalent of a foreign government or international organization.
2	Mild	Expected impact is minor and limited to influence, obstruct, undermine, discredit or disrupt the operations of smaller scale.	Confidential information whose disclosure may be disadvantageous to the Armed Forces or relationship to another state or an international organization or otherwise to

			national security. Secret document that has been given the designation RESTRICTED or equivalent of a foreign government or international organization.
1	Negligible	Consequences for the business are negligible.	Data are not secret or foreign classified.

Table 1: Assessment of the impact according to five-point scale

2.5 Exposure levels

With the level of exposure referred, the assessment of the system is exposed with respect to any actor's ability to influence the system. This opportunity can be both physical that is; anyone can access the technical equipment that forms the system as logical system via various interfaces.

One system's exposure is expressed in four levels with E1 and E4 as the lowest and maximum exposure level. Increased opportunities for any stakeholder to influence the system is defined as a higher level of exposure, which in turn leads to higher demands on the system's security capability.

The criteria for the four exposure levels are shown in Table 2.

Exposure levels are the lowest level for which it is specified for both criteria, i.e. access to the system's physical and logical interfaces and the exchange of information, is satisfied. Note that iterations may be required to identify a cost-effective level, e.g., by changing the conditions of the system and its intended operating environment.

2.5.1 *Exposure from people*

For people who are temporarily staying in the rooms where they can get access to a system's interfaces and should not increase the system exposure level, must be monitored by someone who is deemed reliable for the task and is competent enough to determine what constitutes a risk to the system. See directive on "Personell bevakning" in the letter HKV 2010-06- 23 10.700:60542[21].

[21] HKV 2010-06-23 10 700: 60542 Directive concerning sectioning etc. in the areas of IT and telecommunications

2.5.2 *Exposure from information exchange*

With the information provided in the exchange of information with other IT systems, whether it takes place over an electronic communications network or removable storage media. Introduction of security updates and updating of safety functions' control and their governing data (e.g. antivirus) which takes place in accordance with established operating and safety instructions, does not affect the exposure of the IT system.

At the exchange of information with the systems at the same or lower consistency exposure level, also for the players who can get access to these other systems. To get the claim that such information does not mean increased exposure to the system must be described in detail how the security features of the other systems protects the system from this unwanted possibility exchange can mean.

Note that in the last example, the system can exchange information with a system on a geographically separate location, where several other system forwards the message on the road. In this case, the system must be considered to have information exchange with all the systems that handled the message. This is explained in Example 1 below. Use a signal protection with approved intrusion prevention features, such as a VPN encryption, to exchange information over a carrier, for example, a network, do not need the system is considered exposed to the wearer. This is explained further in Example 2 below.

When assessing the exposure of information with a system that is not subject to accreditation by the Armed Forces so must the system's IT security capabilities assessed. The assessment is made on the basis of existing agreements with the organization that is responsible for the system and their approvals of the system.

Exposure level	Criteria for the exposure level		
	Access to the system's physical and logical interfaces		**Information exchange**
E4	*All cases that do not meet the criteria for any of the exposure levels E1-E3 below.*		*All cases that do not meet the criteria for any of the exposure levels E1-E3 below.*
E3	All people[22] with access to one of the system's interfaces are safety tested[23].	and	All systems that exchange information with the system are accredited to a higher level of consistency or All systems that the system exchanges information with are accredited to the same consistency level with a maximum exposure level E3.
E2	All people with access to one of the system's interfaces are competent to any information for the highest consistency level processed in the system.	and	All systems that exchange information with the system are accredited[24] to a higher level of consistency or All systems that the system exchanges information with are accredited[25] to the same consistency level with a maximum exposure level E2.
E1	All individuals with access to the system's interfaces are responsible[26] for all information processed in the system.	and	The system exchanges no information with other systems.

Table 3: Exposure levels with associated criteria

[22] Foreign personnel (for example, international exercises and operations) are handled separately.
[23] § 14 Security Ordinance (1996:633)
[24] In the case of other organizations handled through contracts and agreements
[25] In the case of other organizations handled through contracts and agreements
[26] Chapter 7. 1 § FIB IT security

Example 1: Determination of the level of exposure

IT system A handles information with consequence level 2 and level of exposure should be assessed. The system is in areas where only authorized people have access to its physical interfaces. The system therefore meets the criteria for the exposure level 2 in terms of exposure to people with access to the system's interfaces. System A, however, exchanges information with the system B that is accredited for consequence level 3 with the exposure level 4. The exchange of information takes place via messages transmitted by the system C and D that are accredited for consequence level 2 with exposure levels 2 and 3 respectively.

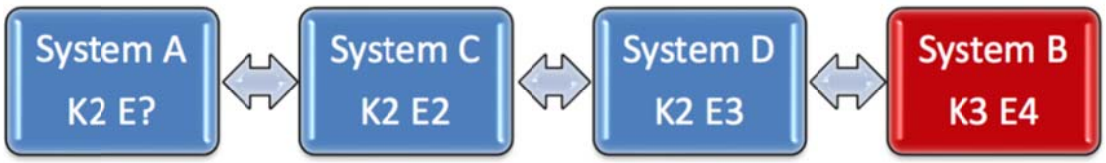

Figure 7: ***Example 1: Determination of the level of exposure***

This means that IT system A is exposed to players who have access to either system B, C or D. Since the system D is accredited for the same consequence level and exposure levels 3, this provides the highest exposure and IT system A is therefore expected to have the exposure level 3.

In this case, however, the system D security features which ensure that the players are a threat to the system can not affect the system A. System A can then describe how that rely on these safety features in System D, and meet when all the criteria for the exposure level 2.

Example 2: Use of approved signal protection as intrusion protection

IT systems X and Y are two systems that handle information with consequence level 2 and share information over a non-accredited network Z. Systems X and Y have no other business exposure that would give a higher level of exposure than E2, but is expected to have the exposure level 4 due to the exposure from the network Z.

Figure 8: ***Example 2 - Exchange of information through non-accredited network***

By dividing the systems X and Y in each of two subsystems X1, X2 and Y1, Y2, where X1 and Y1 consists only of a signal protection component with approved intrusion protection properties may subsystems X2 and Y2 describe how they rely on intrusion protection signal protection components of X1 and Y1 offers and can be evaluated for exposure level E2 as they would have received if they had not communicated via network Z.

Figure 9: ***Example 2 - Information exchange through approved signal protection as intrusion protection***

As this is expected to be a common scenario permitted by the KSF an exception in the assessment of exposure levels where the system has information via signal protection with approved intrusion prevention characteristics need not deemed exposed to signal protection system "carriers" and thus allowed to reach the lower levels of exposure without performing the above described division into subsystems.

2.6 Determination of the level of requirements

Security requirements are divided into three levels: Basic (G), Extended (U) and High (H). The requirements are determined based on the consequence level, i.e. consequence of information loss, and system exposure level.

The table below indicates the level of requirements for functional safety and assurance requirements. Identified requirement level constitutes the input value for further work on requirements and components as demonstrated by in Appendix 3 for the functional safety requirements and in Annex 4 for the assurance requirements.

Consequence level	Exposure level			
	E1	E2	E3	E4
5	H	H	H	H
4	U	H	H	H
3	U	U	U	H
2	G	U	U	U
1	G	G	G	G

Table 4: Requirement levels of functional safety and assurance requirements

2.7 Documentation – ITSS

For each system, an IT security specification (ITSS) is developed that describes the system, its intended use and the analysis performed to determine the information consequence level and the system level of exposure. A ITSS shall also contain all safety requirements for the system, both those given by KSF and those given by business analysis and safety analysis. ITSS is the requirements specification for IT security that the system is verified against. The structure and content of ITSS is determined by the KSF and is described in Annex 2 to this document. If parts of the content that is in demand in ITSS already exist in other documents, it is sufficient that the ITSS give an unambiguous reference to the information.

In order to verify that the system meets its ITSS, different types of documentation and evidence such as design documents, test plans, test results, documentation of procedures for version control and operation of the system are required. What documentation is required and what information should appear is determined by the assurance requirements.

Except for ITSS, KSF sets no requirements for size or appearance on these surfaces other than that it is established and includes that which is required by the assurance requirements.

2.8 Evaluation

The assessment that a system meets KSF, i.e. that the system meets all the security requirements and that you have enough confidence in this, is called the KSF evaluation. The methodology for this is described in KSF Evaluation manual and it is a separate document. In any assurance requirements provided that the system developer to produce certain documentation to demonstrate confidence in the

system's security capability and the KSF Evaluation manual is the description of how this material should be reviewed.

4 Assurance requirements

4.1 Introduction

Assurance requirements are the requirements for confidence in the system's ability to provide its security functionality. Assurance requirements are divided into different classes covering different assurance areas and requiring different kind of information. **The increasing level of requirements is also placing the increasing demands on the scope of the law, completeness and degree of detail.** It is this material that will be then verified during the evaluation process.

4.2 Structure of the assurance requirements

In the category assurance requirements there are following seven classes of requirements, which are described in detail in Annex 4:

- IT Security Specification (SASS) - Because it is a prerequisite for the evaluation of other classes of assurance requirements that the system ITSS is true, complete and consistent, makes this class of requirement designed to ensure this.
- System development life cycle (SALC) - This class includes assurance requirements on safety-relevant characteristics in the development environment, such as physical environment, the components' origin and processes for the development and maintenance of the environment where the system develops.
- Architecture and Design (SADE) - This class includes assurance requirements on technical characteristics of the IT system design and construction, i.e. characteristics of the system and the documentation of them.
- Installation and operation (SHOP) - This class includes assurance requirements for documentation, processes and procedures used in the operation and management of the system for the system to work safely.
- Administrative procedures (SARU) includes assurance requirements on the documentation that the developer produces and which describes how the systems system's security features should be administered in a proper way to maintain the system's IT security skills.
- System Integration Test (SATS) - This class includes assurance requirements for system testing, which shows that the system developer verified the IT security functionality of the system.

- Vulnerability Assessment and Residual Risk Assessment (SARA) - This class covers the vulnerability assessment conducted by the evaluator, largely based on the material from other assurance families.

4.3 Component Assurance

A system consists of a combination of one or more IT components, where some of these contribute to security functionality. An IT component is security-related if it is used to fulfill a safety function or if it provides functionality on which the security function depends on. As confidence in these IT components safety skills is vital for the confidence of the entire system, it is part of the IT system assurance requirements to determine which components of a particular system are security-related. For the other (non-safety related) components is required an amount equal to that described in the document HKV 2007-08-23 10,750: 7,210,027, or a complete reference to such components. The level of assurance required by the safety related IT components called component assurance level and described in four levels from Level 1 to Level 4 (N1-N4) where level 4 is the highest level of assurance. The process for approving security-related IT components to specific component assurance level is an independent process that is outside KSF.

The table bellow is used for exploratory purposes describing the overall difference between the different levels. The contents in the table below should not be confused with the identification of specific requirement.

Level	The overall differences between the component assurance level
N4	MUST can approve products, which completely aim to fulfill IT security requirements to N4. The development of the product shall be according to a formal project methodology with clear milestones, such as MIL-STD-1521B. Furthermore, MUST must evaluate and approve the requirements, demands interpretation, architecture, development, design, development, product testing and final delivery items.
N3	MUST can approve products whose functionality wholly or mainly aims to meet the IT security requirements to N3. Alternatively, the product can be as modular security functionality that can be easily defined and evaluated in isolation. Component developer shall assist the audit with everything the reviewer needs, such as documentation and access to relevant resources, such as staff and test environment. Component developer shall demonstrate that all the work, regarding the product, is controlled by a comprehensive security process, which includes the entire product life cycle.
N2	MUST can approve IT security functions in the general COTS (Commercial Off The Shelf) products to N2. This requires that the component developer provides

	sufficient information to support the review. An example of such information is thorough documentation of the product, source product, documentation of the developer's tests and reports of the safety reviews carried out by third parties. Component developer shall demonstrate that the product is developed and maintained according to a documented safety process that covers the entire product life cycle.
N1	MUST approve IT security functions in the general COTS (Commercial Off The Shelf) products to N1. This requires sufficient documentation that defines the security function and its interfaces. Dependencies of the functions in and outside of the product must also be described. Component developer should demonstrate good safety awareness in his/her handling of the product life cycle.

Table 5: Overall difference between component assurance levels.

MUST verifies the IT security functionality of IT components and approves of any of these four component assurance levels.

4.4 Determination of component assurance level

The requirement of component assurance level, within the safety related IT components in a system, is controlled by the highest consequence level of information and the system level of exposure.

	Exposure level			
Consequence level	*E1*	*E2*	*E3*	*E4*
K5	N2	N3	N4	N4
K4	N2	N2	N4	N4
K4	N2	N2	N3	N4
K2	N1	N2	N2	N3
K1	N1	N1	N1	N1

Table 6: Component assurance level

When the various security components of a system are exposed to different exposure or used to protect information that has different consequence level, then the component assurance level does not have to be as high for all the security component in the system.

A safety component with lower component assurance level can be used if it shows that the component has a lower exposure than the system maximum, or alternatively only protects the information on a lower consequence level than the system's highest. This may require the presence of any IT security component of higher component assurance level that guarantees that. However, some characteristics of the system architecture can allow the use of components with lower component assurance level.

System developer should identify the system's security related components. If a component with lower component assurance level than what is given in the table above is used in the system, the system developer has to demonstrate why this does not affect the security negatively. This should be documented in ITSS and will be reviewed and evaluated during the evaluation of the system.

Example 1. Component of higher assurance gives lower exposure

A system has an architecture that allows a division into two parts. All communication between these elements is done through a filter that allows only text files. One part has a greater amount of users and exposure E4. The other part has only a few users who are all competent to all the information covered there. Then the components that implement malware protection in the smaller system could be assigned to the component assurance level given exposure level E2. Component assurance level for other components in the system would not be reduced in this case. For example, components that realize authentication still have exposure level E4, then the filter in this example can not determine who is allowed to send the text files through it. In addition, an analysis will be made to ensure that all traffic actually goes through the filter and that there are no other routes into the malware.

Example 2. Information of higher consequence level is kept in a separate part of the system

Information of high consequence level is kept in a separate part of the system and protected by a component that emits only information of the lower level of consequence. Component assurance level of the components in the rest of the system would be reduced on the grounds that they do not handle the information on the higher level of consistency.

The requirement level of the IT system as a whole and the component that implements the protection of information on the higher consequence level will be guided by the information at the highest level of consequence and not be lowered.

To achieve an efficient architecture, the system and its safety features are designed and placed in such a way that it can be shown that information with maximum protection will only be handled and protected by components that meet sufficiently high standards for this purpose. In this way you reach a system architecture adapted to the business which are not the highest consistency level affects all parts of the system and thereby reach a cost-effective protection.

Example 3. The system architecture affects exposure

Even properties in the system architecture can affect component assurance level. A system can be linked to two other systems with different exposure levels and protected by two different intrusion detection components to each system. According to the method for determining component assurance level would be a component that implements intrusion towards the lower exposed the system to have a lower component assurance level than the other intrusion protection.

Appendix B: KSF v3.1: IT System Security Specification (ITSS)

KSF

Requirements for IT security capabilities of IT systems

v3.1

IT System Security Specification (ITSS)

TABLE OF CONTENTS

1 General strategy

1.1 The purpose of ITSS

IT system security specification (ITSS) specifies which IT security abilities system to have, and in what way and in what environment they will be used for the system to be considered safe enough and the system's safety features and operating environment work together to ensure these IT security abilities. To reach this objective, the following must stand:

- IT system architecture, its operating environment and its logical and physical limits described.
- IT system functional safety requirements and assurance requirements identified based on KSF security model by evaluating the system's consequence level and exposure.
- Additional safety requirements are identified based on business requirements, identified threats and risks as well as regulatory requirements.
- Safety requirements for the operational environment are identified based on business requirements, identified threats and risks as well as regulatory requirements. If some KSF requirements are claimed to be fully or partly met by utilizing the characteristics of the environment, they should also be documented as safety requirements for the operational environment.
- Security features that fully satisfy the system's security requirements are documented.

1.2 Intended use

ITSS can be used during the requirements definition, development, evaluation and accreditation of the system and when the system becomes operational. ITSS is thus a common safety specification for different parties such as clients, providers, evaluators and users.

- Requirements definition

Armed Forces (the client) have to use ITSS to have the overall picture of the safety requirements for the system and its environment, and thus to be sure that the provider shares the overall picture and that is verified by evaluator. Safety requirements image consists of the applicable KSF requirements and other additional safety and security following the operational environment.

- IT system development

The executor must implement all identified safety requirements for the system and document in the ITSS how these requirements are met.

- Accreditation

Evaluation will verify the system meets its ITSS. Evaluation should verify that ITSS is accurate, complete, clear and non-contradictory, and that it corresponds to the actual requirements picture.

- Drift

The Armed Forces shall administer ITP and document how the security picture as described in ITSS affected over time[1]. ITSS and especially the safety requirements for its operational environment will provide a basis for the development of local procedures and instructions for system operation and personnel management.

2 ITSS obligatory content

The mandatory contents of an ITSS presented in Figure 1 "ITSS structure". Each chapter of ITSS described briefly below and more fully described in the following sub-chapters.

- In *Introduction*, ITSS and system uniquely identified and references to the KSF and any other documents or security standards that the system must meet. Introduction also provides a comprehensive and accurate high-level description of the system.
- In *System Description* a detailed description of the system is provided. The description defines system requirements, architecture, interfaces, and security capabilities.
- In *Summary of safety requirements*, safety requirements of the system are described. These safety requirements are identified based on KSF security model and security analysis, business analysis, threat, risk and vulnerability assessment and constitutional analysis of the specific system.
- In *Safety requirements on environment*, safety requirements for operational environment are described. These safety requirements are identified based on security analysis, business analysis, threat, risk and vulnerability assessment and constitutional analysis of the specific system. KSF requirements can be argued to be fully or partly met by utilizing the characteristics of the operational environment and this is documented as safety requirements for the operational environment.
- In *Interpretation of safety*, a compiled set of requirements for the system is described. For all functional safety requirements documented in chapter “Summary of security”, it is described how these are applied to the specific system. The safety of the system's operating environment is referred to some KSF requirements and can be argued to be, totally or partially, fulfilled by utilizing the characteristics of the operating environment.
- In *Compliance with security requirements* is given a complete high-level description of the security measures implemented in the system. It also shows how these measures meet the specific security requirements of the system's security features.

[1] Description of and requirements for any ITSS management is not included in the KSF.

2.1 Introduction

2.1.1 Objective

The Introduction provides a comprehensive and accurate high-level description of the system.

The purpose of this chapter is to give an overview of the system. An overview of the system shall contain information about the system's intended use and its security functionality of the system.

The description of how ITSS meets various safety requirements and regulations must be expressed clearly in this chapter. This is important for the following reasons:

- the reader should be able to identify (track) requirements,
- the provider must show that the system has been built for specific safety and
- the evaluator must determine whether safety requirements are met

2.1.2 Content and presentation

The chapter will provide an overview of the system from the following aspects:

(a) ITSS reference:

ITSS should contain a clear reference that uniquely identifies ITSS. A typical reference may contain title, version, authors and publication date e.g. "ITSS, v1.2 system XYZ, Developed by ABC AB, 2014-06-09".

(b) IT system reference:

ITSS will also include a system’s reference that uniquely identifies the system. IT system’s reference shall be the same as used in the Armed Forces IT process.

(c) Document references:

ITSS shall include references to the KSF and other governing documents and international standards. The references must demonstrate that ITSS acceptably represent KSF requirements governing documents, international standards (e.g., FIPS 180-3, RFC 425), and other safety standards (e.g. EU directive NATO standards) system shall meet.

Document references in ITSS should reference the exact version of the document and any level of requirements the system must meet, such "KSF v3.1 Requirement level U".

It should also be specified on the system or its IT components meet all safety requirements in the standard, or only meet the standard for some elements (such as FIPS 180-3 only for SHA-256 ").

(d) System overview:

System overview briefly describes the use and security mechanisms and system architecture. The description should provide an overview of the system's IT security capacity and its intended use. The intended operating environment for the system is also described. Any technical or environmental factor that the system is dependent to will be included in the description.

2.2 System description

2.2.1 Objective

System description provides a detailed description of the system. The description should provide the accrediting system and the system user capacity and manage a deeper understanding of security capability in the system than is given in the chapter *Introduction*.

System description describes the system requirements, architecture, interfaces, and security capabilities:

- Safety relevant information about the system prerequisites must be reported to the appropriate level of requirements for the system to be established, thus must show:
    - Intended use of the system, that is, the business support it provides
    - How its operating environment is constituted, for example, regarding the physical protection of the system
    - Which are the intended users of the system
    - What information is stored, transferred and processed in the system
- IT system architecture must list all components and describe how they together make up the system.
- IT system’s all logical and physical interfaces should be described to give a picture of the attack surface they represent.
- IT system security skills should be described in a level of detail that is sufficient to give the reader a general understanding of these. The description is expected to be more detailed than that given in the chapter Introduction.

Having the system architecture and security capabilities described is of the utmost importance, in a way that it is clear which parts belong to the system and which are external dependencies.

2.2.2 Content and presentation

Description of the system consists of four parts: conditions, architecture, interfaces and security capabilities.

(a) Conditions

To describe the system operating conditions it is necessary to define

- Intended use of the system

This is a description of the intended use of the system from the user's perspective in terms of processing, storage and transmission of information.

- System’s operating environment

Here the system's placement in the operating environment is described with information on physical protection, access restriction and other conditions that are relevant to safety.

- Intended users of the system

This part of the system intended users is described. All user roles in the system will be reported and the possible grouping of users for access to resources and information to be identified. For each user role, its level of access to the system's various security features and other safety-relevant assets are listed. The number of users in each role and the group will also be assessed so that the reader understands the system's scope.

- Information

Type of information, quantity, value protection, classification, possible other handling rules (e.g. from regulatory requirements) on the information stored, processed, transmitted or carried out of the system. A reference to the system's safety should also be given.

(b) System architecture

In order to identify the safety of the system it is necessary to specify the overall system architecture.

Architectural description shall identify the components and describe how they interact. The information should be presented in sufficient detail to give the reader a general knowledge of how the system operates and the general flow of information available.

(c) System interfaces

IT system’s all logical and physical interfaces should be identified and described. The description shall, in addition to the definition of interfaces and physical location, identify what information is supposed to be exchanged at the interface and how the exchange is supposed to take place.

Reference to it, or they, component(s) in the architecture description that constitute the interface, and any components that are designed to protect the interface or control the exchange of information above shall also be given.

(d) Security capabilities

While the system architecture describes the system architecture and the components included in the system, this describes the system's security capabilities and security features provided by the system. Safety faculties described at a level of detail that is sufficient to give the reader a general understanding.

2.3 Summary of safety requirements

2.3.1 Objective

The purpose of the compilation of safety is to identify the safety requirements of the system. The safety requirements can be divided into two categories:

- KSF requirements

The KSF security model takes into account the system consequence level and exposure to reach a level of requirements. KSF security model is described in KSF main document, Chapter 2.

- Additional safety

Additional safety requirements are those requirements that have been identified outside KSF's security model, e.g. as a result of various mandatory analyses performed. These analyses can identify additional safety requirements on the system or its operating environment. The safety requirements for the system shall be documented in this chapter, while the security requirements that must be met by operational environment must be documented in chapter Safety on the surroundings.

2.3.2 Content and presentation

Summary of security consists of two parts: KSF requirements and additional safety requirements.

(a) KSF requirements

KSF requirements define two types of safety requirements: functional safety requirements and assurance requirements.

To identify KSF requirements that apply to a system, a method for setting the level of requirements is applied. This method is described in KSF main document, Chapter 3. The requirements are used in the SEF are:

- Basic IT security (G)
- Advanced IT security protection (U)
- High IT security protection (H)

The result of the determination of the level of requirements must be documented and all requirements components resulting from the level of requirements to be listed in this chapter.

(b) Additional safety requirements

Additional safety requirements are derived from analyses outside KSF security model. Methods for conducting such analyses are not included in the KSF. Methods for the implementation of operational and safety are described in the H SÄK Infosäk[2]. Methods of threat, risk and vulnerability are described in the Armed Forces common risk management model[3]. Other analyses may result in safety requirements on the system, e.g. from safety requirements, processing of personal data or other regulations and statutes.

These analyses will identify measurable safety objectives for the system or its environment obtained based on identified threats, management requirements and regulatory requirements. These safety objectives for the system are to be compared with the safety requirements stemming from the KSF and documented as additional safety requirements. If the safety objectives are already covered by the safety of the KSF, the reference to those safety requirements are documented. Safety objectives identified for the system's environment should also be listed as requirements in chapter Safety requirements on the surroundings.

2.4 Safety requirements on environment

2.4.1 *Objective*

The purpose of the safety requirements on the environment is to identify the safety requirements of the operational environment. These requirements can arise when KSF requirements of security mechanisms in the system environment but can also be identified through analysis outside KSF security model.

These analyzes identify safety of the system and its environment. Safety objectives for the system reported in the previous chapter Summary of safety.

Some KSF requirements or requirements components can be argued to be fully or partly met by relying on the characteristics of the operational environment. These can be physical, administrative and organizational measures. The measures cited will then be the safety of its operational environment.

[2] Guide Information Security 2013 M7739-352056
[3] Armed Forces Joint Risk Management Model 2009 M7739-350012

2.4.2 Content and presentation

Identified security objectives together with actions in the operating environment and any KSF requirements or demands components, thereby deemed to be satisfied to be documented.

The documentation should include a list of all the security requirements of the system operating environment must meet, so that this can be used for verification during system commissioning.

2.5 Interpretation of safety

2.5.1 Objective

The purpose of Interpretation of security requirements is to describe a compiled set of requirements for the system and to implement and document requirements interpretation based on the security requirements identified in the chapter Summary of safety. The requirements of the KSF formulated at a general level that results in each system needs to specify these requirements with an interpretation of the requirement applied to the system.

The analyses described in chapter Safety on the environment can identify some KSF requirements can be argued to be met by utilizing the characteristics of the operational environment. If KSF requirements or requirements components, to be followed by the safety of the environment, the reference to the safety of the environment indicated in requirement interpretation.

2.5.2 Content and presentation

Interpretation of security requirements shall describe a compiled set of requirements for the system.

All security requirements should be documented in order to produce a consolidated set of requirements in the ITSS. The requirements to be used as the basis for system design to realize the security requirements.

The following requirements interpretations are allowed:

- Specification

Clarification means that safety requirements are documented in the Chapter Summary of security requirements that shall be described in terms applicable to a specific system. A specified requirement will be more stringent than the original KSF- requirements.

- Reference to the safety of the environment

Reference to the safety of the environment should be given for the KSF requirements or demands components that can be argued to be met by utilizing the characteristics of the operational environment. These requirements are identified in chapter Safety on the surroundings.

2.6 Compliance with security requirements

2.6.1 Objective

The purpose of the Compliance with security requirements is to give a description of how the system fulfils the safety requirements imposed on the system. It should contain a description of the components and safety features that meet functional safety requirements on the system. How assurance requirements need not be described. Neither the functional requirements are met by the system environment needs to be described.

The information should be presented in sufficient detail so that the reader can ascertain how all the functional safety requirements.

The identification of KSF requirements and additional safety requirements described in the section Summary of safety. How these identified KSF requirements specified for a specific system is described in the Interpretation of safety.

2.6.2 Content and presentation

Compliance with security requirements should show all of the requirements listed in the chapter Interpretation of the safety requirements of the system. This is done by describing the security functionality of the system designed to meet every requirement. Evaluation should be based on this description, and with the support of the system description, to ensure that all safety requirements are fully met by the system.

If a component with lower component assurance level than that provided by the system's consequence level and exposure level (see Chapter 4 of the main document) is used in the system, that should be specially motivated and exporter must clearly show that this can not affect the safety of the system negatively.

Appendix C: KSF v3.1: Assurance Requirements

KSF

Requirements for IT security capabilities of IT systems

v3.1

Assurance Requirements

TABLE OF CONTENTS

1 Assurance model for IT system

The purpose of assurance requirements is to have confidence that the system meets the IT security abilities that KSF demands. This is achieved by ensuring:

- confidence in the system developer and his development,
- confidence in the architecture, design and implementation of security features,
- confidence in the operation and that administration documentation is accurate and complete,
- through vulnerability assessment and risk analysis to demonstrate that the system for the intended use, has sufficient IT security abilities.

Assurance requirements have two aspects:

- Only required data from the system developer that describes the design, testing and administrative procedures, as well as evidence showing that these procedures are followed and that tests have been performed.
- It then looks at the basis of the evaluator that checks if the base is full, clear and non-contradictory. It then analyses the system of evaluator, inter alia testing, to find possible vulnerabilities. Any residual risks are identified and described, so that an accreditation can be judged to be acceptable or not.

The model is based on the system that is composed of components with known security capabilities and reports any uncertainties. The model relies that these security capabilities are known and documented through processes that verified these components.

Below is a summary of the various assurance classes:

- Confidence in IT security specification (SASS) includes assurance requirements of ITSS[1]. SASS requires ITSS format and content to ensure that ITSS is accurate, complete, clear and not contradictory to be a suitable specification for a system that will meet the KSF.
- System development life cycle (SALC) includes assurance requirements for security in the development environment. Development environment refers to the environment in which the system evolved, or is integrated into, not the environment in which the components have been developed. This is done by imposing requirements on the description of the system developer's

[1] The system's IT security specification

control of the components and other safety measures in the development environment. The demands on the version and configuration management, life cycle model for system development, system delivery to the operating and management systems, and how the developer will take care of discovered security flaws in the system or its components.

- Architecture and Design (SADE) includes assurance requirements on security architecture and the descriptions of how components provide security functionality. This is done by making demands on an architecture description that will show how the various components work together to provide the overall safety functionality of the system. The design shall also describe how information worth protecting is flowing in the system so that you can verify that it can be protected. The design will also show how the system that prevents the security functionality can be bypassed or manipulated. Finally, the architecture and design show external interfaces available to the environment and the degree to which the system relies on the operating environment.
- Installation and operation (SAOP) includes assurance requirements for documentation, processes and procedures that are used when operating and management to install and manage the system. This is done by imposing requirements on the description of the proposed management that ensures that the system has been controlled in delivery and installed in its operating environment according to the system developer's instructions. The assurance also includes requirements for documentation that should contain all information necessary for the system to be operated and maintained safely.
- Administrative procedures (SARU) include assurance requirements for the documentation that the system developer produces and describing how the system's security features should be administered in a proper way to maintain the system's IT security skills.
- System Integration Test (SATS) includes assurance requirements on the system developer testing. This is done by imposing requirements on the description of the tests conducted to show that there are test cases for all functional requirements and security functions. Functional tests must show that the tests carried out and the results properly documented.
- Risk Analysis and Vulnerability Assessment (SARA) includes assurance requirements on identification and documentation of possible anomalies, vulnerabilities and residual risks to assess and manage them. This is done by making demands on the system developer's description of identified deviations. In addition, a vulnerability assessment carried out by the evaluators show that no identified vulnerabilities could be exploited. Any residual risks identified by evaluator during the risk analysis should be documented.

2 Assurance requirements

2.1 SASS - The system's IT security specification

The purpose of this class is to have confidence that the system's IT security specification (ITSS) is suitable as a specification for a scheme evaluation. This is done by examining whether ITSS correctly applied the KSF security model to determine the level of safety; the ITSS is technically sound, non-contradictory and has made a correct interpretation of safety requirements. Whether the system can meet these security requirements are taken care of all other systems assurance requirements.

The class SASS consists of six requirements:

- Introduction (SASS_INL) comprises ITSS chapter Introduction to ensure that the introduction uniquely identifies a particular version of ITSS, and refers to a specific version of the system and the version of the KSF, and that it contains a comprehensive and accurate high-level description of the system.
- System description (SASS_SYS) comprises ITSS chapter System description to ensure that the system description should give a detailed description of the system and that the information used to determine the level of requirements based on KSF security model is documented.
- Summary of safety (SASS_KRV) comprises ITSS chapter Compilation of safety to ensure that all security requirements for the system are correctly identified on the basis of KSF model or from other external requirements.
- Safety on the environment (SASS_OMG) includes ITSS chapter Safety on the environment to ensure that all security requirements for the system environment are identified and described.
- Interpretation of safety (SASS_TOL) comprises ITSS chapter Interpretation of security to ensure that the description shows a complete set of requirements for the system and define requirements KSF interpretation based on the requirements identified in the ITSS section Summary of safety.
- Compliance with security requirements (SASS_UPF) includes ITSS Compliance with security to ensure that all functional safety requirements identified are handled by the system.

SASS_INL - ITSS Introduction

The requirement includes the Introduction of ITSS provides a comprehensive and accurate description of the system that includes the following:

- A reference that identifies ITSS.
- A reference that identifies the system and showing that ITSS acceptably represent KSF and other requirements document that the system meets.
- A system overview that briefly describes the use of the system, architecture, and security features.

The following table shows the components requirements applicable at the respective level of requirements:

SASS_INL	D1	C1	C2	C3	C4	C5	C6	C7	E1
Basic	X	X	X	X	X	X	X	X	X
Extended	X	X	X	X	X	X	X	X	X
High	X	X	X	X	X	X	X	X	X

SASS_INL.D1

The developer will provide an Introduction

SASS_INL.C1

The introduction should consist of ITSS-reference system reference and system overview

SASS_INL.C2

ITSS reference should clearly identify ITSS

SASS_INL.C3

IT system reference should clearly identify the system

SASS_INL.C4

IT system reference SHOUL identify the version of the KSF requirements and the requirement level, which ITSS indicates that the system must meet.

SASS_INL.C5

IT system reference should identify normative documents, international standards and other security documents ITSS enter the system to meet

SASS_INL.C6

IT system reference should show which safety requirements in the current requirements collection; the system and its components shall meet

SASS_INL.C7

System Overview will describe the use and security mechanisms in the system at a high level

SASS_INL.E1

Evaluator should verify that the information in the dossier meets all requirements for content and presentation

SASS_SYS - System Description

The requirement applies to the description of the system in the ITSS. It must describe the system in such a way that the system description can identify KSF requirements, but also to understand how the system will be used and how it interacts with its environment. Thus, the conditions for the system, its architecture, interfaces and security capabilities must be described.

The following table shows the components requirements applicable at the respective level of requirements:

SASS_SYS	D1	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	E1
Basic	X	X	X	X	X	X	X	X	X	X	X	X	X
Extended	X	X	X	X	X	X	X	X	X	X	X	X	X
High	X	X	X	X	X	X	X	X	X	X	X	X	X

SASS_SYS.D1

The system developer shall provide a System Description

SASS_SYS.C1

The system description should describe what information is handled in the system and the consequences that could arise from the loss of this information

SASS_SYS.C2

The system description should describe the system's exposure

SASS_SYS.C3

Description of information, consistency and system exposure should be done with terms that KSF use and that enable KSF requirements can be based on these factors

SASS_SYS.C4

The system description should describe the system's intended use, users of the system and information to be stored, processed, transmitted or carried out of the system

SASS_SYS.C5

The system description should describe the system's physical boundaries, and all externally accessible interfaces

SASS_SYS.C6

The system description shall describe the purpose and method of use for all externally accessible interfaces

SASS_SYS.C7

The system description should describe the system architecture and design, and to identify the components that the system consists of

SASS_SYS.C8

The system description shall clearly identify the components that are relevant to safety

SASS_SYS.C9

The system description must for all externally accessible interfaces include a description of the individual components that comprise the interface

SASS_SYS.C10

The system description should describe the system's security capabilities and security features provided by the system

SASS_SYS.C11

The description of the system's abilities must be clear, consistent and agreeable with other parts of ITSS

SASS_SYS.E1

Evaluator should verify that the information in the dossier meets all requirements for content and presentation

SASS_KRV - Compilation of safety

This requirement includes the compilation of all the system's security requirements documented in ITSS compilation of safety. These safety requirements on the system are identified based on KSF security model and other analyses that must be performed. It should show that the KSF security model is applied in accordance with chapter System description and all functional safety requirements and assurance requirements identified and documented. It will also show not only that security requirements have been identified, but that all safety requirements either based in the KSF model or has been identified by other analyses and requirements standings.

The following table shows the components requirements applicable at the respective level of requirements:

SASS_KRV	D1	C1	C2	C3	C4	C5	C6	E1
Basic	X	X	X	X	X	X	X	X
Extended	X	X	X	X	X	X	X	X
High	X	X	X	X	X	X	X	X

SASS_KRV.D1

The system developer shall provide a summary of safety

SASS_KRV.C1

The compilation of security requirements shall identify the requirements that come from the KSF and the requirements for future safety requirements

SASS_KRV.C2

The compilation of KSF requirements shall describe the level of requirements for all requirements, all applicable requirements thereof components, both those that are met by the system and those that must be met by the system environment

SASS_KRV.C3

The compilation of KSF requirements should describe the requirement level of assurance requirements and all applicable requirements components

SASS_KRV.C4

Additional security requirements shall identify all security objectives identified in other analyzes carried out (as compulsory business analysis, security analysis, threat, risk and vulnerability, and constitutional analysis)

SASS_KRV.C5

The description of the KSF requirements and additional safety requirements should identify the requirements to be met by the system and which should be met by the system environment

SASS_KRV.C6

The description of the KSF requirements and future functional requirements should be clear, consistent and agreeable with other parts of ITSS

SASS_KRV.E1

Evaluator should verify that the information in the dossier meets all requirements for content and presentation

SASS_OMG - Safety on the environment

This requirement shall demonstrate that the conditions for the system environment and safety requirements that are on systems environment documented. Some security requirements for the system are supposed to be fully or partly met by utilizing the system's environment. These safety requirements must be documented how and to what degree they are supposed to be met by safety requirements on the environment, with a level of detail equivalent to safety requirements of requirements' components.

The chapter will show that all the necessary conditions on the system environment are identified and that all safety requirements of the system environment are identified and documented. These

conditions should be formulated as to the safety of the environment so that they can be unambiguously put into the system environment.

The following table shows the components requirements applicable at the respective level of requirements:

SASS_OMG	D1	C1	C2	C3	C4	C5	E1
Basic	X	X	X	X	X	X	X
Extended	X	X	X	X	X	X	X
High	X	X	X	X	X	X	X

SASS_OMG.D1

The system developer shall provide Safety requirements on environment

SASS_OMG.C1

The safety of the environment shall identify and describe all the conditions on the system environment necessary for the system to meet their security requirements

SASS_OMG.C2

The safety of the environment shall describe the physical, administrative and organizational measures in the system's environment that fully or partially meet the safety requirements for the system's environment

SASS_OMG.C3

The safety of the environment shall identify security requirements and the functional safety of the system derived from KSF and partly or wholly disposed of the system's environment

SASS_OMG.C4

The description of the safety requirements for the system's environment will clearly show what requirements are met by the system and which are met by the system's environment

SASS_OMG.C5

The description of the safety requirements for the system's environment to be clear, consistent and consistent with other parts of ITSS

SASS_OMG.E1

Evaluator should verify that the information in the dossier meets all requirements for content and presentation

SASS_TOL - Interpretation of safety

This requirement means that the safety of the system must be interpreted (decomposed) at a system-specific way so that they can concretely translated by the system. Then the functional safety requirements of the KSF is formulated at a general level that make them generally useful, you must specify the security requirements for each system in order to describe a compiled set of requirements for the system. The interpretation of the safety requirements should be so clear-cut that it can be used as a basis for system design. The interpretation of safety is to show that KSF requirements specified. This means that evaluator must verify whether the precise KSF- requirement is stricter than the original SEF requirement.

It may be that certain functional requirements are met to a certain part of the system and some of its surroundings, in any interaction between the system and its environment. This interpretation of the requirements must be such that they uniquely identify the requirements for the system and the requirements applicable to its environment.

Note: Even assurance requirements must be interpreted, but this interpretation does not affect the system's design and implementation, but the interpretation is done continuously during the development process.

The following table shows the components requirements applicable at the respective level of requirements:

SASS_TOL	D1	C1	C2	C3	C4	E1
Basic	X	X	X	X	X	X
Extended	X	X	X	X	X	X
High	X	X	X	X	X	X

SASS_TOL.D1

The system developer shall provide an interpretation of safety

SASS_TOL.C1

The interpretation of security requirements shall describe the interpretation of all of the safety requirements for the system

SASS_TOL.C2

The interpretation of safety requirements shall specify the functional safety requirements so that they interpreted the requirements are testable and that a design can be verified against the interpretation of the requirement

SASS_TOL.C3

The interpretation of safety requirements must be as strict or stricter than the original requirements, whether the requirements coming from the KSF or additional safety

SASS_TOL.C4

The description of the interpretation of the KSF requirements and additional safety requirements should be clear, consistent and consistent with other parts of ITSS

SASS_TOL.E1

Evaluator should verify that the information in the dossier meets all requirements for content and presentation

SASS_UPF - Compliance with security requirements

This requirement means that compliance with security requirements should demonstrate that all interpreted the requirements of the system shall be met by the identified safety functionality of the system. All requirements must be met and only security functionality that meets the requirements to be described. Security functionality that meets the security requirements must comply with the system description.

The following table shows the components requirements applicable at the respective level of requirements:

SASS_UPF	D1	C1	C2	C3	C4	E1
Basic	X	X	X	X	X	X
Extended	X	X	X	X	X	X
High	X	X	X	X	X	X

SASS_UPF.D1

The system developer shall provide Compliance with security requirements

SASS_UPF.C1

Compliance with security requirements should show how all the safety requirements in the chapter Interpretation of the safety requirements have been met by the system security features

SASS_UPF.C2

Compliance with security requirements should demonstrate that all requirements are met entirely by the system

SASS_UPF.C3

Compliance with safety requirements for each requirement shall show that all requirements have been met by the system

SASS_UPF.C4

The description of the fulfilment of the safety requirements should be clear, consistent and agreeable with other parts of ITSS

SASS_UPF.E1

Evaluator should verify that the information in the dossier meets all requirements for content and presentation

2.2 SALC - System Development Life Cycle

The purpose of this class is to gain confidence in the system developer's management of system from design, through system development and integration to delivery. The first prerequisite is to have confidence in the origin of the system and its components, to ensure that the system developer manages the system and its components in a way that changes in these only occur under controlled conditions.

SALC differ on whether the system is in component developer, systems developer or operating and managing the organization's control.

The responsibility and control of the system is considered to follow the steps below:

1. During the development of the system, ie before the system is complete and has been delivered, the system is under the developer's control systems.

2. When the system is ready and has been delivered and accepted, responsibility and thereby controls the operation and management.

3. The management of the system begins, which usually involves both systems developer and the operation and management. Fixed security flaws (eg system updates) developed and distributed to the operation and management must have processes to handle system updates so as to verify and install them. SALC includes only system developer's part of it; requirements for the operation and management of the system described in the class SAOP.

SALC does not include the development of the components included in the system. In SALC are included demands for the handling of components in the system's life cycle, when they left the component developer's control and is under the developer's control system, until the system is shipped to the operation and management.

The requirements on component development are included in the component assurance requirements and verified through the approval process for components. This also applies in cases where the system developer himself develops some of the components.

The class SALC consists of five requirements:

- The security of the system development and integration environment (SALC_UTV) covers systems developer's control of the components, systems developer's physical, administrative (procedures), personnel and other security measures to maintain the security of the system during its development.

- Version and configuration management (SALC_KFG) is concerned with the scope and procedures for version control and configuration management of the components or parts that are included in the system. As to show that changes in the system are performed by authorized persons in a controlled manner.
- Delivery (SALC_LEV) covers the procedures that the system developer uses to ensure that the delivery to the operation and management is done in a safe manner. It means to prevent or detect privacy or loss that could lead to deficiencies in the system's security capability.
- The life-cycle model (SALC_LCM) covers life cycle model for system development and maintenance of the system developer, so as to have confidence that the system's quality.
- Lack Correction (SALC_BRK) covers the process and procedures for the detected safety-related defects in the system and its components are taken care of and reported to the customer. It also includes how the system developer handles the safety-related deficiencies detected and reported by the component developer for the components included in the system.

SALC_UTV - Development Safety

This requirement addresses the security of the development and integration environment. The requirement focuses on the where the components and systems come from, the security of the development environment, personal and physical security but also access to critical information that could affect confidence in the system. When a system can consist of components from multiple vendors it must also have control of the supply chain for these components. A component should only be integrated into a system after having undergone an acceptance procedure that will ensure confidence in the supply chain.

At higher assurance requirements, more extensive and in-depth control mechanisms of the system developer for the development environment, acceptance procedures and the supply chain are required.

Note: This requirement is based on the existence of a trust for the system developer. How this is to be determined is outside KSF and is not handled by SALC_UTV. In some cases, the criteria for this depend on the system, e.g. depending on how the system is used and which information to be protected.

The following table shows the components requirements applicable at the respective level of requirements:

SALC_UTV	D1	D2	D3	D4	C1	C2	C3	C4	C5	C6	E1	E2
Basic												
Extended	X	X	X	X	X	X	X	X			X	X
High	X	X	X	X	X	X			X	X	X	X

SALC_UTV.D1

The system developer shall provide system documentation

SALC_UTV.D2

System developer must apply system development documentation

SALC_UTV.D3

The system developer shall provide integration documentation

SALC_UTV.D4

The system developer shall provide acceptance criteria for components that will be included in the system

SALC_UTV.C1

System documentation shall describe the physical, logical, administrative, personnel and other security measures necessary to ensure the privacy and accuracy of the design and implementation of the system in the development environment

SALC_UTV.C2

System documentation shall demonstrate that the security measures provide an accurate protection of the development environment, which is at least on par with the protection system, will offer

SALC_UTV.C3

The acceptance criteria should describe sufficient criteria for acceptance and verification of safety-related components included in the system

SALC_UTV.C4

Integration documentation shall identify the origins of all component safety-related components and document the origin was identified and how the acceptance inspection took place

SALC_UTV.C5

The acceptance criteria should describe sufficient criteria for acceptance and verification of all IT components included in the system

SALC_UTV.C6

Integration documentation shall identify the origins of all the components and document that the origin was identified and how the acceptance inspection took place

SALC_UTV.E1

Evaluator should verify that the information in the dossier meets all requirements for content and presentation

SALC UTV.E2

Evaluator should verify that the system documentation applies security measures

SALC_KFG - Configuration Management

This requirement includes routines for version control and configuration management to prevent unauthorized or accidental alteration of configuration-controlled components. System developer must have documented procedures and mechanisms that provide protection for accuracy in the development and maintenance of systems and components. In order to uniquely identify a system, each component is recorded in a configuration management system. For each system it must also be able to identify out of which components it consists.

The production will be using the configuration management system to demonstrate that the delivered system is identical to the tested and approved. In software can configuration management be handled using automated tools.

Complex systems often consist also of hardware components. In these cases shall also relevant information for identifying the hardware including software be found in the configuration management system. This may be e.g. model numbers and versions.

All systems should be followed up with the exact version of the components so that the security amendments related to the versions of the components can be made and monitored. A configuration management system to support change management so that it is implemented in a verifiable manner and by qualified personnel.

The following table shows the components requirements applicable at the respective level of requirements:

SALC_KFG	D1	D2	D2	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	E1	E2
Basic															
Extended	X	X	X	X	X	X	X	X	X	X	X	X		X	X
High	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

SALC_KFG.D1

The system developer shall provide system and a unique system reference

SALC_KFG.D2

System developer will use a configuration management system

SALC_KFG.D3

The system developer shall provide documentation describing the configuration management system

SALC_KFG.C1

IT system and its components must be marked with a unique reference

SALC_KFG.C2

The documentation describing the configuration management will demonstrate methods for unique identification of configuration-driven IT components

SALC_KFG.C3

The documentation describing the configuration management will demonstrate how configuration management used in system development and system developer's management of the system

SALC_KFG.C4

All configuration items included in the system will be under configuration management

SALC_KFG.C5

The documentation describing the configuration management should describe the acceptance procedures for new and updated configuration items

SALC_KFG.C6

The documentation describing the configuration management must demonstrate the acceptance procedures used provides adequate change management for all configuration items

SALC_KFG.C7

Documentation must demonstrate that the system for configuration management is conducted in the legality of the documentation of configuration management

SALC_KFG.C8

Documentation must demonstrate that all components and its parts, all assurance documents, reports of potential safety and other documentation that describes the provider's management of the system is under the control of configuration management

SALC_KFG.C9

Configuration management system shall provide safety measures for change management that ensures that all changes are implemented in a controlled manner and by qualified personnel

SALC_KFG.C10

Configuration management system shall include the technical features for traceability that ensures that all changes can clearly be traced to the individual who conducted them

SALC_KFG.E1

Evaluation should verify that the information in the dossier meets all requirements for content and presentation

SALC_KFG.E2

Evaluator should verify that the configuration management system applies security measures

SALC_LEV - Delivery System

This requirement includes procedures for the delivery process to prevent and detect manipulation, privacy loss or other damage that can lead to the system's security capability not being maintained. System developer must have documented procedures and mechanisms that provide this protection and which allows the receiver before installation and commissioning to verify that no tampering occurred. Thus the aim is to ensure the controlled delivery of a certain audited and approved system for operation and management.

It may be that a system, especially if it is a large, complex and distributed system, consists of components that are distributed in different ways to different places. In such cases, subject to all these modes of supply of SALC_LEV.

SALC_LEV requires documented procedures that describe how the system protects the user from the developer to deploy a system that åverkats during delivery and therefore can not be considered safe.

The following table shows the components requirements applicable at the respective level of requirements:

SALC_LEV	D1	D2	C1	C2	C3	E1
Basic	X	X	X	X		X
Extended	X	X	X	X	X	X
High	X	X	X	X	X	X

SALC_LEV.D1

The system developer shall provide documentation describing the procedures and mechanisms for the IT system and component deliveries

SALC_LEV.D2

System developer shall use the delivery procedures

SALC_LEV.C1

Delivery documentation shall describe all procedures that are necessary to maintain the security of the system during its delivery to the operating and management organization

SALC_LEV.C2

Delivery documentation shall describe how the system's accuracy is protected during delivery

SALC_LEV.C3

Delivery documentation shall describe how the system accuracy can be verified by the recipient upon delivery and at any time after delivery

SALC_LEV.E1

Evaluator should verify that the information in the dossier meets all requirements for content and presentation

SALC_LCM - Lifecycle Model

This requirement includes the life cycle model for system development. Basic elements of a life cycle model are test and acceptance procedures in the design, development and delivery phases of a system.

In integrating the components from one or more suppliers to the life cycle model defining the acceptance procedures required.

A life-cycle model encompasses procedures, tools and techniques to develop and maintain a system. Examples of components of such a model are the design methods, systems developer's own audit processes, project management models, procedures for change management, testing and acceptance procedures. An efficient life cycle model takes into account all these aspects in a common management model with explicit responsibilities and follow-up.

The following table shows the components requirements applicable at the respective level of requirements:

SALC_LCM	D1	D2	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	E1	E2
Basic														
Extended	X	X	X	X	X	X	X	X	X	X			X	X

High	X	X	X	X	X	X	X	X	X	X	X	X	X	X

SALC_LCM.D1

System developer shall establish a life-cycle model to be used in the development of the system and the system developer's management of the system

SALC_LCM.D2

System developer must provide documentation that describes the life cycle model

SALC_LCM.C1

The life-cycle model should include systems development and systems developer's management of the system

SALC_LCM.C2

The life-cycle model shall provide control over system development and system developer's management of the system

SALC_LCM.C3

The life-cycle model shall describe the need to assess the security impact of changes in the system during the system's life cycle.

SALC_LCM.C4

The life-cycle model will describe the need to maintain the security of the system during its life cycle and systems developer's management of the system

SALC_LCM.C5

The life-cycle model will describe the parts of the design, operation and management documentation necessary to maintain security during the system's life cycle

SALC_LCM.C6

The life-cycle model will describe procedures for verification of suitability for use in the system

SALC_LCM.C7

The life-cycle model will describe the acceptance and release procedures for system design and the components

SALC_LCM.C8

The life-cycle model will describe how quality is integrated into the system life cycle

SALC_LCM.C9

The life-cycle model will describe how the process of quality assurance meets similar requirements of ISO 9001

SALC_LCM.C10

The procedures for verification of suitability for use of the system shall include the judgment of each component security impact on system

SALC_LCM.E1

Evaluation should verify that the information in the dossier meets all requirements for content and presentation

SALC_LCM.E2

Evaluator should verify that the life cycle model is applied

SALC_BRK - Lack Correction

This requirement includes the detected safety-related defects in the delivered system handled. The requirements cover the entire lifecycle of a safety-related deficiencies, how and where it is reported, the information provided to the operation and management, the process of how the deficiency is rectified and the system is updated.

These assurance requirements however do not place requirement on system developer's ability to detect various safety-related deficiencies.

Some safety-related deficiencies cannot be repaired immediately, and other alternative measures should be taken.

If the system is developed and implemented by the system developer but agreements regulate the operation and management organization will manage the administration of the system without continuing support from the system developer can this requirement be deleted. In such cases, transferred responsibility for the lack correction to the operational and administrative structures and systems developer must provide adequate instructions for this in order to maintain system security. The requirement for this material is in the class SAOP (SAOP_BRK).

The following table shows the components requirements applicable at the respective level of requirements:

SALC_BRK	D1	D2	D3	D4	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	E1
Basic	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Extended	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
High	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

SALC_BRK.D1

The system developer shall provide documented procedures for the handling of safety-related defects in the system

SALC_BRK.D2

System developer should have the necessary agreements and processes to get information about the safety-relevant flaws in the system and components

SALC_BRK.D3

The system developer shall provide operational and administrative documentation of safety-related defects in the system

SALC_BRK.D4

System developer should establish a process for reporting safety-related defects in the system

SALC_BRK.C1

Operating and managing documentation shall describe how the operational and administrative organization can report suspected safety-related defects in the system

SALC_BRK.C2

Operation and management documentation shall identify specific contact for all reports and inquiries about security-relevant flaws in the system

SALC_BRK.C3

Documented procedures for the management of safety-related defects in the system shall describe methods for the safe delivery of information about the shortcomings and lack patch and security updates to the operating and management organization

SALC_BRK.C4

Documented procedures for the management of safety-related defects in the system shall ensure that corrective actions are identified for all known safety-related deficiencies

SALC_BRK.C5

The documentation describing the handling of safety-related deficiencies shall describe how the information about the shortcomings and instructions on remedies provided operating and management organization

SALC_BRK.C6

Documented procedures for the management of safety-related defects in the system shall ensure that all known safety-related deficiencies are remedied and that security updates are issued to the operating and management organization

SALC_BRK.C7

Documented procedures for the management of safety-related defects in the system to ensure that security updates do not introduce any new security flaws or deficiencies in functionality

SALC_BRK.C8

The documentation describing the handling of safety-related deficiencies shall describe the procedures used to track all reported security flaws in relevant system in every release

SALC_BRK.C9

The documentation describing the handling of safety-related deficiencies shall describe how the operational and administrative documentation categorize the nature and effect of each security relevant shortage and the status of corrective actions

SALC_BRK.C10

Documented procedures for the management of safety-related defects in the system to ensure that all components are integrated in the process of handling safety-relevant flaws in the system

SALC_BRK.E1

Evaluator should verify that the information in the dossier meets all requirements for content and presentation

2.3 SADE - Architecture and Design

The purpose of this class is to achieve that confidence in the system's architecture and design is well described and not contradictory. It must also be shown that the architecture and the individual components provide the security functionality and assurance listed in ITSS.

When the security architecture and design documentation are primarily two qualities that are important:

- Safety functionality should be clearly identified in the architecture and safety features must be specified.
- The IT system should not be used in such a way that the security functionality can be manipulated or circumvented.

The class SADE consists of four requirements:

- Interface description (SADE_GRÄ) covers requirements for description of the purpose and usage of the system's external interfaces.
- Security architecture (SADE_ARK) includes requirements for architecture description that the system developer must provide.
- Data flow analysis (SADE_DFA) includes requirements for the identification of the components that store and process critical[2] data.
- Design documentation (SADE_DES) covers requirements for description of all safety-relevant components and how these contribute to the security capabilities to meet the system's safety.

SADE_GRÄ - Interface description

This requirement includes the identification and description of the system's external interfaces to understand how external entities, such as users or other systems interact with the system and the risks involved. All external interfaces are identified and described to the point that their safety relevance and impact of the measures taken can be determined.

---

[2] Critical data is either worthy of protection itself or data which may affect the protection of such data

External communication with other systems must be described in such a way that you can verify the documentation, such as programming guides, describing how other systems should be programmed and configured to be able to safely interact with the system.

In addition, the description of the external interfaces provides sufficient information so that the vulnerability analysis understands the attack surface that the system exhibits. For this to be possible, for each interface it should be indicated the degree to which the interface is exposed to specific attacks, based on attack scenarios and the attacker's capacity or potential attack and why the interface for specific reasons, such as assumptions about the environment, can not be subjected to a given attack.

The following table shows the components requirements applicable at the respective level of requirements:

SADE_GRÄ	D1	C1	C2	C3	C4	E1
Basic						
Extended	X	X	X	X	X	X
High	X	X	X	X	X	X

SADE_GRÄ.D1
The system developer shall provide a description of system interfaces

SADE_GRÄ.C1
The description of the system's interfaces should include an analysis of which externally accessible interfaces are safety-relevant and which are not

SADE_GRÄ.C2
The description of the system's interfaces should contain a description of the safety standpoint, relevant actions associated with each safety-relevant interface.

SADE_GRÄ.C3

The description of the system's interfaces should include a summary of the security features that are associated with the respective interface

SADE_GRÄ.C4

The description of the system's interfaces should include complete description of the interaction system all externally accessible interfaces allow.

SADE_GRÄ.E1

Evaluator should verify that the information in the dossier meets all requirements for content and presentation

SADE_ARK - Security architecture

This requirement means that the system developer must provide a description of the system security architecture that will show how the components contribute to the security of the system and also safety critical dependencies between components. The description of the architecture shall contain the information needed to determine the degree to which the architecture is dependent on the specific components and its characteristics.

Assurance level components must be specified so that the trust relationships that rely on components assurance are documented in architecture. In order to permit assessment of the architectural soundness and accuracy, shall protection for the information stored or processed on different components be recognized and boundaries between various security requirements identified. The description of the architecture must also include the system's ability to protect itself from manipulation of the security functionality and the attempt to circumvent the security features.

The main goal of this requirement is to verify that the system's security architecture is sound and right. There are dependencies to the design description that can affect the level of detail required in the architecture description. The evaluation of SADE_ARK therefore needs to be made in connection with SADE_GRÄ and SADE_DES.

The following table shows the components requirements applicable at the respective level of requirements:

SADE_ARK	D1	D2	C1	C2	C3	E1	E2
Basic							

Extended	X	X	X	X	X	X	X
High	X	X	X	X	X	X	X

SADE_ARK.D1

The system developer shall provide a description of the system security architecture

SADE_ARK.D2

System developer will design and implement the system so that the security features cannot be bypassed

SADE_ARK.C1

The description of the security architecture should demonstrate how the components go together and their interactions result in system security functionality

SADE_ARK.C2

The security architecture must for every safety-relevant component identify other components that it depends on and how it depends on the other components

SADE_ARK.C3

The description of the security architecture should demonstrate that the system architecture prevents security functionality to be bypassed

SADE_ARK.E1

Evaluation should verify that the information in the dossier meets all requirements for content and presentation

SADE_ARK.E2

Evaluator should analyze the surface and verify that it is not possible to bypass the system's security features

SADE_DFA - Data Flow Analysis

Data flow analysis deals with the identification of the components that store and process critical data. A system has various components that handle a variety of data, although all data is not critical. In

order to ensure that proper safeguards are used to protect critical data, systems developer provides a test that shows where in the system critical data is stored and processed. The analysis forms the basis of assurance profiling and systems developer's risk analysis.

The following table shows the components requirements applicable at the respective level of requirements:

SADE_DFA	D1	C1	C2	C3	C4	C5	E1
Basic							
Extended	X	X	X	X	X		X
High	X	X	X	X	X	X	X

SADE_DF A.D1

The system developer shall provide a data flow analysis of critical data in the system

SADE_DF A.C1

Data flow analysis shall identify all critical data stored and processed by the system

SADE_DF A.C2

Data flow analysis must include an impact assessment of the level of the critical data stored or processed by components of the system

SADE_DF A.C3

Data flow analysis will document the components that store or process-critical data as well as the components that do not process or store critical data

SADE_DF A.C4

Data flow analysis will document how critical data is transferred between components in the system

SADE_DF A.C5

Data flow analysis must consider all the data critical and therefore fully describe the all system data flows

SADE_DF A.E1

Evaluator should verify that the information in the dossier meets all requirements for content and

presentation

SADE_DES - Design Documentation

This requirement addresses how each component contributes to the security functionality to the system, and how components are integrated into the system. While SADE_ARK provides a view of the architecture perspective, i.e. architectural requirements for components, giving SADE_DES a komponentvy, i.e. how the components contribute to the architecture.

A design description (SADE_DES) is expressed in terms of the logical components of the system that provides a more comprehensive service or function. If in a system, for example, includes a firewall, design description of this would include the actions performed by the firewall when a packet arrives.

A component description is part of the design of the system and provides a high-level description of what a particular part of the system does and how it works.

The purpose of the design documentation is to provide enough information to determine the boundaries of components that add security capabilities of the system and how the security functions implement the safety requirements on the system. The scope and structure of the design documentation depends on the complexity of the system, the number of components and the safety features they implement.

The following table shows the components requirements applicable at the respective level of requirements:

SADE_DES	D1	C1	C2	C3	C4	C5	C6	E1
Basic								
Extended	X	X	X	X	X	X		X
High	X	X	X	X	X	X	X	X

SADE_DES.D1

Systems developer shall provide design documentation for the system

SADE_DES.C1

The design shall describe the structure of the system in terms of its components

SADE_DES.C2

The design shall identify all components that contribute to the security functionality of the system

SADE_DES.C3

The design shall describe each component's behavior sufficiently to determine what components are safety-relevant

SADE_DES.C4

The design should include a description of the interaction between the safety-relevant components and between safety-related and non-safety-relevant components

SADE_DES.C5

Design documentation shall demonstrate that any externally accessible interface identified in the interfacial description is associated with at least one safety-relevant component

SADE_DES.C6

Design documentation shall demonstrate fully how the system components and their configuration give the system its intended IT security abilities

SADE_DES.E1

Evaluator should verify that the information in the dossier meets all requirements for content and presentation

2.4 SAOP - Installation and operation

The purpose of this class is to ensure that the system can be installed, deployed, administered and maintained in a safe manner.

Systems developer is responsible for providing full, clear and not contradictory operation and management documentation system. This may mean that the special operation and administration documentation needs to be developed for specific configurations or environments. To ensure that system security is maintained throughout the system life cycle must be enclosed operating and administrative records containing sufficient information required for the operation and management personnel to implement their part of fault management process when the system is operating and

managing the organization's control.

The class SAOP consists of three requirements:

- Installation and preparation (SAOP_INS) includes a requirement that the system should be received and installed in its operating environment safely.
- Operating and administrative documentation (SAOP_DOK) covers requirements for written policies and procedures to be used by all kinds of operational and administrative staff who are expected to be.
- Lack Correction (SAOP_BRK) includes requirements for procedures and conditions for deficiency correction system.

SAOP_INS - Installation and preparation

This requirement will ensure that the system will be received and installed in its operating environment safely and as systems developer intended. This includes examining whether the system could be configured or installed in an unsafe manner while the system's operation and management organization feel that it is safe.

The first process covered by the preparatory action are operating and managing the organization's acceptance that the delivered system is not tampered with. The control is performed in accordance with the system developer's instructions. An installed system will also meet the security objectives for the operational environment. This may include: physical protection, RÖS-protection mm. For systems delivered as several separate components, these requirements apply to all parts of the system and for each delivery.

The following table shows the components requirements applicable at the respective level of requirements:

SAOP_INS	D1	C1	C2	C3	C4	E1	E2
Basic	X	X	X	X		X	
Extended	X	X	X	X	X	X	X
High	X	X	X	X	X	X	X

SAOP_INS.D1

The system developer shall provide the system with documentation describing the preparatory actions

SAOP_INS.C1

The preparatory actions should describe all the steps necessary to safely accept the delivered system in accordance with the developer's delivery system procedure (SALC_LEV)

SAOP_INS.C2

The preparatory actions must describe all necessary steps for the safe installation of the system

SAOP_INS.C3

The preparatory actions should include steps to ensure that the operating environment meets the requirements of the operating environment as documented in ITSS (SASS_OMG)

SAOP_INS.C4

The preparatory actions should include steps for verification of correct installation

SAOP_INS.E1

Evaluation should verify that the information in the dossier meets all requirements for content and presentation

SAOP_INS.E2

Evaluator shall implement measures to verify that the system can be received and installed safely by following the description of them

SAOP_DOK - Operating and administrative documentation

This requirement means that the operating and management documentation must contain the information necessary for the system to operate in a safe manner, in accordance with the system developer's intentions. Requirements are also imposed on the operation and administration documentation that is not misleading or deceptive, which may lead to misuse of the system.

Operating and administrative documentation shall describe the security functionality of the system and provide instructions (including warnings) to the operating and management personnel to understand the system's security capabilities. Operation and management documentation includes safety-related

measures and the information necessary for the system to be used safely.

The goal of this is to reduce the risk of human or other errors that could disable, switch off or obstruct the security functionality.

The following table shows the components requirements applicable at the respective level of requirements:

SAOP_DOK	D1	C1	C2	C3	C4	C5	C6	C7	C8	E1
Basic	X	X	X	X	X	X	X	X	X	X
Extended	X	X	X	X	X	X	X	X	X	X
High	X	X	X	X	X	X	X	X	X	X

SAOP_DOK.D1

The system developer shall provide operational and administrative documentation

SAOP_DOK.C1

Operating and administrative documentation shall, for each user role, describe the user interface and security features available to the user

SAOP_DOK.C2

Operating and administrative documentation shall, for each user role, describe how the available user interface provided by the system to be used safely. This includes all the safety parameters that the user can change and what values they can consider safe

SAOP_DOK.C3

Operating and administrative documentation shall, for each user role, clearly describe each type of security-relevant activity related to the user available actions that must perform extensive operation and maintenance of the security features

SAOP_DOK.C4

Operating and administrative documentation shall identify all possible modes of operation of the system, including operation after the fault occurred if the system ends up in an uncertain situation, its consequences and implications for the continued safe operation of the system

SAOP_DOK.C5

Operating and administrative documentation shall describe all security requirements that the system and its components have on the environment and other components that are managed by the operating environment of each user role

SAOP_DOK.C6

Operating and administrative documentation shall, for each user role documenting all allowable system configuration critical dependencies between the components configurations

SAOP_DOK.C7

Operating and administrative documentation shall describe procedures for reporting security events, such as loss of equipment or cleared security attributes

SAOP_DOK.C8

Operating and administrative documentation shall be clear and appropriate for the intended users

SAOP_DOK.E1

Evaluator should verify that the information in the dossier meets all requirements for content and presentation

SAOP_BRK - Lack Correction

This requirement will ensure that the operation and management organization has the potential to receive and implement measures to manage safety-related defects in the system. Normally, this means that the instructions for the shortcomings are identified; the developer received them from the system and how they are implemented in the system.

If the system is developed and implemented by the system developer but agreements regulating the operation and management organization shall carry out the management of the system without continuing support from the system developer, the operation and management organization assumes responsibility for the lack of security and lack correction systems developer for the security of the system is to be maintained. These instructions must then be more extensive, and then it should be possible for operational and administrative structures to monitor the information on the defects in the components themselves and obtain information on correcting the deficiencies detected.

The following table shows the components requirements applicable at the respective level of requirements:

SAOP_BRK	D1	D2	C1	C2	C3	C4	C5	C6	C7	C8	E1
Basic	X	X	X	X	X	X	X	X	X	X	X
Extended	X	X	X	X	X	X	X	X	X	X	X
High	X	X	X	X	X	X	X	X	X	X	X

SAOP_BRK.D1

The system developer shall provide instructions that enable operational and administrative organization to carry out monitoring of the shortcomings and lack correction

SAOP_BRK.D2

System developer shall make the necessary contacts to operating and management organization for lack correction information for the system components to be monitored

SAOP_BRK.C1

The instructions should include processes for monitoring sources of information on safety-related defects in the system and its components

SAOP_BRK.C2

The instructions should include processes so that safety-related deficiencies are followed up and corrected

SAOP_BRK.C3

The instructions should describe how the monitoring of safety-related deficiencies shall be documented and demonstrate that the documentation should contain sources, analysis, conclusion and recommended actions

SAOP_BRK.C4

The instructions should include processes for the integration of security updates in the system, including the uninstall

SAOP_BRK.C5

The instructions shall include methods for safe receipt of lack information and a lack correction of the system and its components

SAOP_BRK.C6

The instructions should include procedures for the verification of the existence and origin of security updates before they enter the system

SAOP_BRK.C7

The life-cycle model should include procedures to determine whether a deficiency rectified in a component security is relevant and should be introduced and how it will be accepted

SAOP_BRK.C8

The instructions shall include procedures for testing security updates to ensure that the security functionality is still intact after the introduction

SAOP_BRK.E1

Evaluator should verify that the information in the dossier meets all requirements for content and presentation

2.5 SARU - Administrative procedures

The purpose of this class is to verify that the documentation produced by the system developer includes all the administrative procedures required for the system's security functions to be administered in a proper way. This is needed to ensure that the system is used in the way intended when the system developer designed and implemented security features so that the right IT security abilities of the system are obtained.

The class SARU consists of 6 requirements:

- Requirements on procedures for the allocation and revocation of access rights (SARU_BEH)
- Requirements on procedures for the quality of security attributes for authentication (SARU_ATT)
- Requirements on procedures to detect and track intrusion and abuse in the system (SARU_INT)
- Requirements on procedures for security updates of the system that must be done

(SARU_UPD)

- Requirements on procedures for configuration management of a system (SARU_KON)
- Requirements on procedures for security training of users (SARU_UTB)

SARU_ÅTK - Access Rights

This requirement will ensure that the administrative procedures describing all the necessary information required for the administration of user rights.

The following table shows the components requirements applicable at the respective level of requirements:

SARU_ATK	D1	C1	C2	C3	C4	C5	C6	C7	C8	C9	E1
Basic	X	X	X	X	X	X					X
Extended	X	X	X	X	X	X	X	X		X	X
High	X	X	X	X	X	X	X	X	X	X	X

SARU_ÅTK.D1

The system developer shall provide documented administrative procedures for the allocation and revocation of access rights

SARU_ÅTK.C1

The procedures shall describe how access rights are assigned and revoked

SARU_ÅTK.C2

The procedures shall show access rights as a general rule assigned to roles (or groups) and describe the cases where specific access rights may need to be assigned directly to the subject

SARU_ÅTK.C3

The procedures shall show that user or subject is only assigned to the roles (and groups) that they are authorized to, and necessary for their service

SARU_ÅTK.C4

The procedures shall describe how the follow-up of the assignment is made to ensure that the system users and subjects have been properly assigned roles and access rights

SARU_ÅTK.C5

The procedures shall describe that only authorized operating personnel are assigned access rights to administrative functions for safety functions, their configuration and management of data

SARU_ÅTK.C6

The procedures shall describe a person may not be assigned access rights to more than one of the following functions or roles:

- administration of access control
- administration of security log
- other operating administration

SARU_ÅTK.C7

The procedures shall describe that a person who is assigned access rights to functions for administration of intrusion protection is not at the same time assigned access rights to initiate information transfers controlled by intrusion protection

SARU_ÅTK.C8

The procedures shall describe that a person may not be assigned access rights to more than one of the following functions or roles:

- administration of identities and security attributes for authentication
- assigning roles and access rights to users or subjects

SARU_ÅTK.C9

The procedures should describe only the person responsible for administration of the security log can be assigned access rights to system security logs

SARU_ÅTK.E1

Evaluator should verify that the information in the dossier meets all requirements for content and presentation

SARU_ATT - Security attribute for authentication

This requirement will ensure that the administrative procedures describe how the quality of security attributes for authentication must be checked.

The following table shows the components requirements applicable at the respective level of requirements:

SARU_ATT	D1	C1	C2	C3	C4	C5	C6	C7	E1
Basic	X	X	X	X	X	X	X	X	X
Extended	X	X	X	X	X	X	X	X	X
High	X	X	X	X	X	X	X	X	X

SARU_ATT.D1

The system developer shall provide documented administrative procedures to control the quality of security attributes used for authentication

SARU_ATT.C1

The procedures should describe a minimum acceptable level of quality for passwords chosen by users

SARU_ATT.C2

The procedures shall describe all the assigned password that are randomly generated and how this happens

SARU_ATT.C3

The procedures shall show that randomly generated passwords always consists of at least 12 characters

SARU ATT.C4

The procedures shall demonstrate that passwords are changed during commissioning of the system and operating with a fixed interval

SARU_ATT.C5

The procedures shall describe the regular updating of certificate revocation lists

SARU_ATT.C6

The procedures shall demonstrate that each user identity in the system can be bound to a specific person

SARU_ATT.C7

The procedures shall describe how the monitoring system subjects should be made to ensure that only authorized users subject has valid security attributes for authentication

SARU ATT.E1

Evaluator should verify that the information in the dossier meets all requirements for content and presentation

SARU_INT - Detect and track intrusion and abuse

This requirement will ensure that the administrative procedures describe all the necessary information needed to detect and track intrusion and abuse in the system.

The following table shows the components requirements applicable at the respective level of requirements:

SARU_INT	D1	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	E1
Basic	X	X	X	X	X	X	X	X	X	X	X	X
Extended	X	X	X	X	X	X	X	X	X	X	X	X
High	X	X	X	X	X	X	X	X	X	X	X	X

SARU_INT.D1

The system developer shall provide documented administrative procedures to detect and track intrusion and abuse in the system

SARU_INT.C1

The procedures shall describe how long the security logs shall be saved and to show that they comply with at least the duration that the current regulations dictate

SARU_INT.C2

The procedures shall describe how and with what regularity the utility based analysis of the events recorded in the security log should be

SARU_INT.C3

The procedures shall describe how analysis of operational error events in the system should be and how it should be documented

SARU_INT.C4

The procedures shall describe how the analysis results are classified and show how the classification decision and the decision on action is documented

SARU_INT.C5

The procedures shall describe the analysis and classification of analyzes results are performed only by a trained operator

SARU_INT.C6

The procedures shall describe how the reports on security events, such as loss of equipment or cleared security attributes should be handled and what measures should be taken

SARU_INT.C7

The procedures shall describe how all identified incidents should be investigated and reported

SARU_INT.C8

The procedures shall describe how backup security log should be done regularly to another storage media

SARU_INT.C9

The procedures shall describe how the backup copy of the security log should be stored and show that it must be kept physically separate from the security log

SARU_INT.C10

The procedures shall describe the analysis results continuing to be managed in accordance with its established IT security plan

SARU_INT.E1

Evaluator should verify that the information in the dossier meets all requirements for content and presentation

SARU_UPD - Security Updates

This requirement shall ensure the procedures describing all the necessary information needed for the operating staff to carry out regular security updates to the system.

The following table shows the components requirements applicable at the respective level of requirements:

SARU_UPD	D1	C1	C2	C3	C4	C5	C6	C7	C8	E1
Basic	X	X	X	X	X	X	X	X	X	X
Extended	X	X	X	X	X	X	X	X	X	X
High	X	X	X	X	X	X	X	X	X	X

SARU_UPD.D1

The system developer shall provide documented administrative procedures to perform regular backups of system

SARU_UPD.C1

The procedures should contain detailed instructions for managing security updates for the entire software in the system

SARU_UPD.C2

The procedures should describe the processes for secure update of the security features that are dependent on external supply of safety mechanisms or governing data

SARU_UPD.C3

The procedures should describe the updates to the safety functions' control mechanisms and their governing data shall be verified for accuracy and origin before entering the system

SARU_UPD.C4

The procedures shall demonstrate that all safety-related defects in the system must be corrected within a documented interval of time from the moment of noticing them

SARU_UPD.C5

The procedures shall describe that the security updates to any components of the system should be introduced as soon as possible after they have been made available

SARU_UPD.C6

The procedures shall describe that the security updates correctness and origin has to be verified before they are introduced into the system

SARU_UPD.C7

The procedures shall describe how compliance with the procedures for lack management and security updates is documented so that checks can be easily implemented

SARU_UPD.C8

The procedures shall describe how the risk minimization measures should be taken immediately after a safety-related system weakness is identified

SARU_UPD.E1

Evaluator shall verify that the information in the dossier meets all requirements for content and presentation

SARU_KFG – Configuration control

This requirement will ensure that the administrative procedures describe all the information necessary for operating personnel to implement configuration management system.

The following table shows the components requirements applicable at the respective level of requirements:

SARU_KFG	D1	C1	C2	C3	C4	C5	E1
Basic	X	X	X	X	X	X	X
Extended	X	X	X	X	X	X	X
High	X	X	X	X	X	X	X

SARU_KFG.D1

The system developer shall provide documented administrative procedures to implement configuration management system

SARU_KFG.C1

The procedures shall describe how the current version and update level for all software in the system shall be documented

SARU_KFG.C2

The procedures shall describe how the current configuration of all components in the system must be documented

SARU_KFG.C3

The procedures shall describe how the periodic inspection of the documentation is consistent with the system to be implemented by the operating staff

SARU_KFG.C4

The procedures shall describe how any changes to the system software and configuration to be decided and documented before implementation

SARU_KFG.C5

The procedures shall describe how changing decisions are documented and show that they should include the reason, purpose and document exactly what changes will be implemented

SARU_KFG.E1

Evaluator shall verify that the information in the dossier meets all requirements for content and presentation

SARU_UTB - Safety training of users

This requirement will ensure that the developer provides the training basis for all the different users of the system. Training basis should be sufficient for the given conditions and provide sufficient skills so that the user can use the system safely. Different training base could be for different users of the system.

The following table shows the components requirements applicable at the respective level of

requirements:

SARU_UTB	D1	D2	C1	C2	C3	C4	C5	E1
Basic	X	X	X	X	X	X	X	X
Extended	X	X	X	X	X	X	X	X
High	X	X	X	X	X	X	X	X

SARU_UTB.D1

The system developer shall provide a basis for training

SARU_UTB.D2

System developer must provide procedures for user training

SARU_UTB.C1

Training basis shall be provided for all types of users of the system

SARU_UTB.C2

Training documentation shall include descriptions of how users should report safety-related incidents and the types of incidents that should be reported

SARU_UTB.C3

Training documentation shall for each type of user specify conditions such as previous knowledge

SARU_UTB.C4

The procedures for training shall specify how training is conducted and how the completed training means that users understands the use and its role in maintaining the system security

SARU_UTB.C5

Procedures for training must show that users should have undergone training successfully before they are given permission to use the system

SARU_UTB.E1

Evaluator shall verify that the information in the dossier meets all requirements for content and presentation

2.6 SATS - System Integration Testing

The purpose of this class is to verify that the system security functionality works as it is described in the ITSS and the security features cannot be bypassed. Verification is done by the system developer's functional testing of the safety functionality (SATS_FUN), and system developer's attacker tests. How thorough the tests must be is given from the requirements of test coverage (SATS_TTK). Evaluation testing (SATS_EVL) gives confidence that the system behaves as specified and meets the system's functional safety requirements through quality assurance of system developer’s testing and own additional tests.

The class SATS consists of four requirements:

- Test coverage (SATS_TTK) includes a requirement that all safety features have been covered by the test and, in particular, all external interfaces and components tested satisfactorily.
- Functional tests (SATS_FUN) covers requirements for the system developer to carry out functional tests of the safety functionality and thus provide confidence that the likelihood of flaws in security functionality is relatively small.
- The attacker tests (SATS_ANG) covers requirements for the system developer to conduct tests of security functionality from attackers perspective in order to show that it cannot be overridden.
- Evaluation testing (SATS_EVL) covers requirements for evaluator to verify the result of (SATS_FUN) and (SATS_ANG).

The requirements for test coverage (SATS_TTK), function tests (SATS_FUN) and attacker tests (SATS_ANG) define the documentation that the system developer must prepare for the testing. Evaluator must not only verify this documentation, but also use this documentation to conduct its own tests as part of evaluation testing (SATS_EVL).

SATS_TTK - Test coverage

This requirement shows that there are test cases that cover all the system functional safety requirements and should therefore include all the components that contribute to the overall safety functionality. This is done by the system developer and shall demonstrate that the test cases correlate

with the requirements, safety features and components that are implemented in accordance with SADE_DES.

The goal is to confirm that all security functional requirements are tested and that the security features and components are tested as described in the design documentation.

The following table shows the components requirements applicable at the respective level of requirements:

SATS_TTK	D1	C1	C2	C3	C4	C5	E1
Basic	X	X					X
Extended	X	X	X	X			X
High	X	X	X	X	X	X	X

SATS_TTK.D1

The system developer shall provide an analysis of the test coverage for functional and attacker tests

SATS_TTK.C1

The analysis shall include a justification for why they performed functional tests and attacker tests are considered sufficient and covers all system security features

SATS_TTK.C2

The analysis shall show how the test cases in the test documentation are consistent with the security functional requirements, security functions and components as described in the design documentation

SATS_TTK.C3

The analysis will show that all the requirements components in all functional safety requirements are tested

SATS_TTK.C4

The analysis will show that all of the system's security functions are tested in all safety-relevant components that implement them

SATS_TTK.C5

The analysis shall demonstrate that all safety-relevant components of safety functionality of the system are tested for all component interfaces

SATS_TTK.E1

Evaluator shall verify that the information in the dossier meets all requirements for content and presentation

SATS_FUN - Functional tests

This requirement means that functional tests of the safety functionality shall be implemented by the system developer to ensure that the security functionality works as specified. Functional tests focus on demonstrating that the requirements for system safety functionality as specified in ITTS are achieved with the components' safety functionality and work as described in the design documentation.

The requirements for test coverage (SATS_TTK) and functional tests (SATS_FUN) define the documentation that the system developer must prepare for the testing. Evaluator must not only verify this documentation, but also use this data to conduct tests as part of evaluation testing (SATS_EVL).

SATS_FUN sets requirement on system developer to provide the test plan, test cases, test results and resources required to repeat the testing suits needs. This is to gain confidence that the tests in the test documentation are carried out and the results are properly documented.

The following table shows the components requirements applicable at the respective level of requirements:

SATS_FUN	D1	D2	D3	C1	C2	C3	C4	C5	E1
Basic	X	X		X	X	X	X	X	X
Extended	X	X	X	X	X	X	X	X	X
High	X	X	X	X	X	X	X	X	X

SATS_FUN.D1

System developers shall test the system and produce the test documentation

SATS_FUN.D2

The system developer shall provide a test report

SATS_FUN.D3

The system developer shall provide test documentation

SATS_FUN.C1

The test report shall include description of how the tests were carried out, testing the overall performance as well as any complaints regarding the outcome of the tests

SATS_FUN.C2

The test documentation shall consist of test plans, expected results and actual results

SATS_FUN.C3

Test plans shall describe the tests to be carried out, and the scenario for each test. The descriptions should be so detailed that the tests can be reproduced

SATS_FUN.C4

The expected result shall describe how a successful test results can be identified and distinguished from a non-successful test results. This should be done for each test case

SATS_FUN.C5

The actual test results shall be consistent with the expected test result

SATS_FUN.E1

Evaluator shall verify that the information in the dossier meets all requirements for content and presentation

SATS_ANG – Attacker tests

This requirement means that tests of security functionality to be implemented by the system developer shall ensure that the security functionality of the system is not going to unduly influence or circumvent. Attacker tests shall give confidence that the likelihood of flaws in security functionality is relatively small.

Attacker tests focus on showing that components' safety functionality not only exists and works, but also that they are integrated into the system in such a way that they cannot be circumvented.

The requirements for test coverage (SATS_TTK) and attacker tests (SATS_ANG) define the documentation that the system developer must prepare for testing. Evaluator must not only verify this documentation, but also use this data to conduct tests as part of evaluation testing (SATS_EVL).

The following table shows the components requirements applicable at the respective level of requirements:

SATS_ANG	D1	D2	D3	C1	C2	C3	C4	C5	E1
Basic	X	X		X	X	X	X	X	X
Extended	X	X	X	X	X	X	X	X	X
High	X	X	X	X	X	X	X	X	X

SATS_ANG.D1

System developers shall test the system and produce test documentation

SATS_ANG.D2

The system developer shall provide a test report

SATS_ANG.D3

The system developer shall provide test documentation

SATS_ANG.C1

The test report shall include description of how the tests were carried out, testing the overall performance as well as any complaints regarding the outcome of the tests

SATS_ANG.C2

The test documentation shall consist of test plans, expected results and actual results

SATS_ANG.C3

Test plans shall describe the tests to be carried out, and the scenario for each test. The descriptions should be so detailed that the tests can be reproduced

SATS_ANG.C4

The expected result shall describe how a successful test results can be identified and distinguished from a non-successful test results. This should be done for each test case

SATS_ANG.C5

The actual test results shall be consistent with the expected test result

SATS_ANG.E1

Evaluator should verify that the information in the dossier meets all requirements for content and presentation

SATS_EVL – Evaluation testing

This requirement applies to the testing that evaluator will implement for a system. Evaluation testing includes both repeating the system developer's functional tests and attacker tests (fully or partially) and to extending these tests (extent and depth) with evaluator's own tests. These expanded tests are meant to supplement, not replace, the system developer's tests in a meaningful way. Evaluation testing must therefore be based on both an analysis of the existing tests of the complexity of the system and its security functionality.

A system is possible for testing only if it is made available to evaluator. This involves not only the system, but also the entire test environment, tools, documentation and test suites. A system and its testing environment may be too large or complex to be transported to evaluator. For these cases, evaluators should be given the opportunity to conduct their tests with the system developer as long as it ensures the transparency and independence of the test result. Components of this requirement increase to the amount of independent testing that evaluator must implement.

The following table shows the components requirements applicable at the respective level of requirements:

SATS_EVL	D1	D2	C1	E1	E2	E3	E4
Basic	X	X	X	X	X		
Extended	X	X	X	X	X	X	X
High	X	X	X	X	X	X	X

SATS_EVL.D1

The system developer shall provide system testing

SATS_EVL.D2

The system developer shall provide corresponding set of test resources as those used by the systems developer for the functional testing

SATS_EVL.C1

The IT system shall be in testable condition

SATS_EVL.E1

Evaluator should verify that the information in the dossier meets all requirements for content and presentation

SATS_EVL.E2

Evaluator shall, if it deems necessary, repeat a representative number systems developer's tests and confirm the system developer’s test results for these test cases

SATS_EVL.E3

Evaluator shall analyse the system developer's test cases and complement them with its own test cases

SATS_EVL.E4

Evaluator shall implement its own test cases, document the results and confirm that the system works according to specifications

2.7 SARA - Risk Analysis and Vulnerability Assessment

The purpose of this class is to identify and evaluate any deviations, vulnerabilities and residual risks to adjudicate and manage, or accept them. System developer shall identify all deviations that will then be verified and analysed by the evaluator. Evaluator must also identify and evaluate vulnerabilities that may exist in the actual use of the system.

A system may contain vulnerabilities either through its construction (design and architecture) or through its use (e.g. risk of misconfiguration). There may also be assurance shortcomings to be identified, which could lead to increased risk of vulnerabilities. Examples of assurance shortcomings are certain components relying on other components whose security is not verified or when a particular approved component is used in different configuration than that verified one.

The class SARA consists of three requirements:

- Deviation analysis (SARA_AVV) covers requirements on the system developer to identify any discrepancies and document them; these deviations are then verified by evaluator.
- Vulnerability assessment (SARA_SBH) covers requirements on evaluators to look for possible vulnerabilities, and for each discovered vulnerability check if it could be used in the system's intended environment.
- Residual Risk Analysis (SARA_RRA) covers requirements for numbness whether deviations (uncertainty) and any identified vulnerabilities in the overall system involves a residual risk that can be considered acceptable or not.

SARA_AVV - Deviation Analysis

This requirement means that safety-relevant deviations from the approved use of the components are identified and described in such a way that the system developer can make up the shortfall with its own measures, such as analysis of the difference between the certified configuration and actual configuration. System developer must demonstrate that the measures are sufficient to ensure that the risk of deviation is accurately described.

The following table shows the components requirements applicable at the respective level of requirements:

SARA_AVV	D1	C1	C2	C3	C4	C5	E1
Basic	X	X	X	X	X	X	X
Extended	X	X	X	X	X	X	X
High	X	X	X	X	X	X	X

SARA_AVV.D1
The system developer shall provide a deviation analysis

SARA_AVV.C1
Deviation analysis should include all deviations from the approved configuration of all system safety-relevant components

SARA_AVV.C2
Deviation analysis should include all deviations from the approval of the intended use of all the system's safety-relevant components

SARA_AVV.C3
Deviation analysis should include all deviations from the approval of the assumptions about the system design for all system safety-relevant components

SARA_AVV.C4
Deviation analysis shall for any deviation show what impact it has and how it has been handled

SARA_AVV.C5

Deviation analysis shall show that the measures taken to deal with the deviations are effective

SARA_AVV.E1

Evaluator shall verify that the information in the dossier meets all requirements for content and presentation

SARA_SBH - Vulnerability Analysis

This requirement means that a vulnerability analysis will be conducted to identify any system vulnerabilities that could be exploited in the operational environment. It is evaluator who will look for vulnerabilities. It is system developer's responsibility to ensure that the system is in a testable condition that enables vulnerability analysis and practical tests to be performed.

Vulnerability analysis is not an isolated evaluation activity for the evaluator, but it is up to evaluator in all other evaluation activities to actively use the information compiled to look for potential vulnerabilities that are later used in vulnerability assessment.

Components in this requirement increase through a greater degree of methodology and formalism in vulnerability assessment that the evaluator shall implement. The meaning of the methodical and semi-formal describes the evaluation methods that the evaluator shall follow.

The following table shows the components requirements applicable at the respective level of requirements:

SARA_SBH	D1	C1	E1	E2	E3	E4	E5	E6	E7
Basic	X	X	X	X	X	X			
Extended	X	X	X	X	X		X		X
High	X	X	X	X	X			X	X

SARA_SBH.D1

The system developer shall provide system testing

SARA_SBH.C1

The IT system shall be in a testable condition

SARA_SBH.E1

Evaluator shall verify that the information in the supplier documentation is sufficient to perform a thorough vulnerability assessment of the entire system

SARA_SBH.E2

Evaluator shall use available sources to supplement the supplier documentation, such as audience vulnerability information

SARA_SBH.E3

Evaluator shall analyze, using the provider's documentation and other available information, the system components and interfaces and map their dependencies in order to identify the attack surface and potential weak points in the architecture

SARA_SBH.E4

Evaluator shall carry out independent vulnerability analysis of the system based on the information architecture and design, operation and management documentation and deviation analysis to identify potential vulnerabilities in the system

SARA_SBH.E5

Evaluator shall implement an independent and methodical vulnerability analysis of the system based on all available information and experience to identify potential vulnerabilities in the system

SARA_SBH.E6

Evaluator shall carry out independent, methodical and semi-formal vulnerability analysis of the system based on all available information and experience to identify potential vulnerabilities in the system

SARA_SBH.E7

Evaluation shall conduct practical tests of the system to determine whether potential vulnerabilities can be exploited in the intended use of the system

SARA_RRA - Residual Risk Analysis

The requirement is intended to identify vulnerabilities and uncertainties for the system's security capabilities. Identified uncertainties should be evaluated together with the remaining vulnerabilities that may be identified during the vulnerability analysis to provide a basis for a numbness of the system.

Residual risk analysis is done exclusively by the evaluator using the basis required for the other assurance requirements; no further documentation or analysis is required by the system developer. This means that the residual risk analysis is done as the last step in a system evaluation.

The following table shows the components requirements applicable at the respective level of requirements:

SARA_RRA	E1	E2	E3
Basic	X	X	X
Extended	X	X	X
High	X	X	X

SARA_RRA.E1

Evaluator shall verify that all other evaluating activities are completed successfully

SARA_RRA.E2

Evaluator shall implement the residual risk analysis to identify remaining uncertainties about the system's IT security skills

SARA_RRA.E3

Evaluator shall document the results of the residual risk analysis in a form and language that is clear and gives the intended recipient of the basis for decisions on accreditation

TRITA-ICT-EX-2016:110