

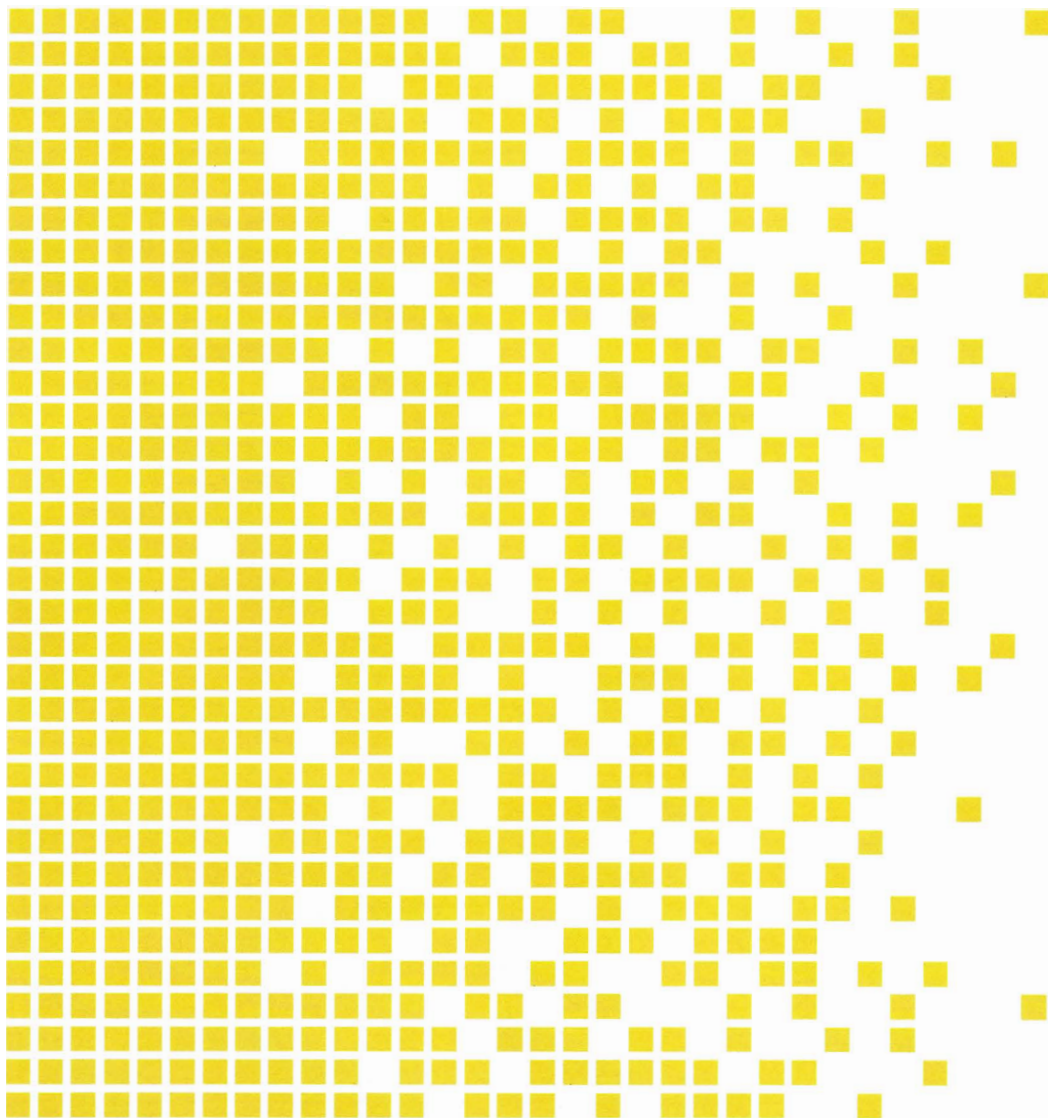


SERTIT

Sertifiseringsmyndigheten for IT-sikkerhet *Norwegian Certification Authority for IT Security*

The Norwegian Certification Scheme

IT Security in Products and Systems

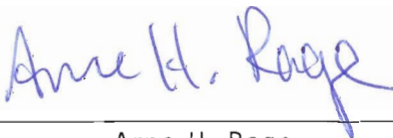



PUBLICATION SD 001E VERSION 9.0 DATE: 02.04.2013

Document History

Document title	The Norwegian Certification Scheme, IT security in products and systems, Sd 001E, Version 9.0, 2 April 2013.
-----------------------	--

Date	Description:
2 April 2013	Published version, 9.0
20 August 2010	Published version, 8.0
28 March 2008	Published version, 7.0
5 July 2007	Published version, 6.0
10 March 2005	Published version, 5.0.
16 September 2004	Published version, 4.0.
1 November 2002	Published version, 3.0.
23 August 2002	Published version, 2.3C.

Last version checked	Last version approved
Kolsås, 02.04.2013	Kolsås. 02.04.2013
 Arne H. Rage	 Kjell W. Bergan
Responsible for Document Control	Head of SERTIT



Contents

1	Overview of the Norwegian Certification Scheme	7
1.1	Background	7
1.2	History	7
1.3	IT security	7
1.4	Challenges	8
1.5	Purpose	9
1.6	Frameworks	9
1.7	Target groups	9
1.8	Security evaluation and certification	10
2	Principles for the Certification Scheme	10
3	Organisation and responsibility	11
3.1	Norwegian National Security Authority (NSM)	11
3.2	SERTIT	11
3.3	Advisory Board	12
3.4	IT Security Evaluation Facilities (ITSEFs)	12
3.5	External parties	12
3.5.1	Sponsors	12
3.5.2	Developers	13
4	General provisions	13
4.1	Conducting security evaluations	13
4.2	Framework conditions for evaluation activities	13
4.3	Rules for publishing information	14
4.4	Complaints, disputes and responses	14
5	Financing of the Certification Scheme	14
6	Preparations for security evaluations	14
6.1	Specification of requirements	15
6.2	Security target	15
6.3	Deliverables	15
6.3.1	Copyright and other rights	16
6.4	Notification of engagements and the security evaluation work plan	16
6.5	Application for certification	16
6.6	Clarifications and commitments	17
6.7	Approval of the certification engagement	17
6.8	Use of consultants	17
6.8.1	Contractual matters	18
7	Security evaluation	19
7.1	Objectives	19
7.2	Implementation	19
7.2.1	Observation reports and journal	19
7.2.2	Interaction	20
7.2.3	Inspection	20

7.3	Evaluation Technical Report	20
7.3.1	Protection of information and protection marking of the ETR	21
7.3.2	Release of the ETR	21
7.3.3	Assessment and approval of the ETR	21
8	Certification	21
8.1	The certification process	22
8.2	Certification Report	22
8.3	Certificate	22
8.3.1	Rights	22
8.3.2	Certified products	22
8.3.3	Use of Certificates	23
8.3.4	Monitoring Certificates	23
8.3.5	Sanctions in the event Certificates are misused	23
9	Maintenance of the Certificate	23
10	Abbreviations	24
11	References	25
Appendix A: Organisation of the Certification Scheme		27
		27
Appendix B: Organisation chart of SERTIT – functions and roles		28
Appendix C: Terms of reference for SERTIT		29

1 Overview of the Norwegian Certification Scheme

This document describes the public scheme for certification of IT security in products and systems. Rules and framework conditions for certification of IT security in products and systems in Norway are drawn up by the *Norwegian Certification Authority for IT Security* (SERTIT). SERTIT is also responsible for certification of IT products and systems.

This document provides an overview of the Certification Scheme, policies, organisation and responsibility, financing, preparations and implementation of security evaluations and finally certification and the maintenance of Certificates.

SERTIT reserves the right to make any changes to the document in the future.

All enquiries concerning this document or comments on its contents shall be addressed to: SERTIT.

1.1 Background

Owing to the rapid developments in IT and the growing use of IT systems for information management in both the public and private sectors as well as by private individuals, the need for independent security evaluation has grown correspondingly.

1.2 History

In autumn 1997 a fact-finding group under the *Norwegian Council for IT Security* prepared a report [22] recommending the establishment of a scheme for certification of IT security in products and systems. The Government decided to establish the Scheme in accordance with the recommendation. Against the background of Proposition No. 1 (1998-99) to the Storting for the Ministry of Trade and Industry, the Storting appropriated funds to the then Headquarters Defence Command Norway/Security Division (CHOD Norway/SEC) for the establishment and operation of SERTIT. As of 1 January 2003 FO/S has become the Norwegian National Security Authority (NSM) a directorate under the Ministry of Defence.

1.3 IT security

To provide an unambiguous understanding of what IT security involves and how it is used in this document, definitions of six key concepts are given below: authenticity, availability, integrity, confidentiality, assurance and accountability. Ref. [8] gives a more complementary definition of information system security and belonging measures.

- **Authenticity** (Ensure that users are identified and authenticated before access to data and services are given, Prevent introduction of false data and services),
- **Availability** (Ensure that information and data resources are available to authorised users at the proper time and in the correct form),

- Integrity (Ensure that the information and data resources is correct and is not altered or destroyed by unauthorised persons),
- Confidentiality (Ensure that the information cannot be accessed by unauthorised persons, and that data resources are protected for unwanted usage),
- Accountability (Ensure that incidents relevant for security are detected and registered, and that users can be kept responsible. This also includes non-repudiation).

In other words, IT security is both measures and policy instruments for protecting information that is stored, processed and communicated in IT systems and protection of data resources. Certification is a method to evaluate and set assurance to IT security. It is this understanding of IT security that applies to this document.

1.4 Challenges

Choosing IT systems to meet specific security requirements calls for an intimate knowledge of the strengths and weaknesses of the various solutions and, not least, access to information about this. Inadequate or misleading information may lead to poor investments or too low IT security.

There are at least three approaches to the evaluation of IT security:

- The first approach is to trust in the supplier's assurances concerning the IT product's or system's qualities and security. However, it often proves on closer examination and testing of the solutions that there are still unsolved security problems and that the IT product or system also has faults and shortcomings. The vendor generally responds by offering fault correction or upgrading, but in the meantime the solution has been operative and information has lacked the required protection.
- The second approach is to conduct one's own tests and evaluations, but such tests are time-consuming and require special expertise. Besides, from a societal standpoint, it is hardly expedient for every purchaser of an IT product or system to have to expend resources on ascertaining whether it satisfies specific functional security requirements and assurance requirements.
- The third approach is to assign the task of assessing the product to an independent third party with the necessary competence. The evaluations are carried out in accordance with internationally recognised criteria and methods, ensuring that all stages of the evaluation process are carried out correctly. From a societal standpoint, this is a more efficient way of ensuring that the IT product or system satisfies the specified requirements because an overall evaluation is carried out while the procurement process for the customers is simplified.

As the purpose of the Certification Scheme is to provide services that support the third approach, the remainder of this document deals exclusively with this approach.

1.5 Purpose

One of the purposes of the Scheme is to meet government and industry sector needs for a cost-effective and efficient security evaluation and certification of IT products and systems.

Therefore, as a party to an international arrangement, cf. sections 1.6, 1.8 and reference [6] and [23], Norway has committed itself to recognising Certificates issued by qualified certification authorities, so-called "Qualified Participants" (QPs). IT products and systems are to be security evaluated and certified in accordance with the international Common Criteria (CC) for evaluation [1], [3] and [4], corresponding to ISO 15408 and the Common Evaluation Methodology (CEM) [5] and [7].

1.6 Frameworks

The Certification Scheme under SERTIT is based on the following international arrangement:

- Arrangement on the Recognition of the Common Criteria Certificates in the field of Information Technology Security (CCRA) [6].
- Mutual Recognition Agreement of Information Technology Security Evaluation Certificates (SOGIS MRA) [23]

In addition, SERTIT has chosen to include the following national documents, which thus form the regulatory framework for the involved parties under the Certification Scheme:

- Act relating to protective security services (the Security Act) [16],
- Regulations relating to data security [8],
- Regulations relating to security classified procurements [9],
- Instructions for handling of documents in need of protection for reasons other than those mentioned in the Security Act with regulations (the Protection Instructions) [12],
- Act relating to the processing of personal data (the Personal Data Act)[15]

All SERTIT documents mentioned in this document or published on SERTIT's website are part of the framework conditions for the Certification Scheme. Changes in these framework conditions will be published in accordance with the current procedures for the Scheme.

1.7 Target groups

Since there is an increasing demand for and growing awareness of the need for IT security in products and systems in society, the impact area for the Scheme is also growing and the target group is therefore broadly composed. The following target groups are key to the Scheme:

- Developers/manufacturers,
- Suppliers/vendors,

- **Buyers/purchasers.**

In addition, those who are to approve IT systems will benefit from the fact that products are certified by an impartial third party. This applies both to actors subject to formal provisions for information security and to actors beyond the scope of security regulations. This includes sectors responsible for systems critical to the society and to business.

1.8 Security evaluation and certification

For all categories of IT users, in the public and private sectors as well as private individuals, it is important to obtain a measure of the requirements satisfied by the system. It is also important to be able to trust that the IT product or system has been subjected to an impartial evaluation by a neutral professional body. This is achieved through the establishment of the Certification Scheme.

Norway is committed to conducting security evaluations and certifications in accordance with internationally recognised standards and methods as they are defined in the CCRA [6] and SOGIS MRA [23].

The CCRA and SOGIS MRA contains two key elements:

- All participants are obliged to recognise Certificates according to the applied rules in the CCRA and SOGIS MRA respectively,
- Recognition of qualified certification bodies, "*Qualified Participants (QPs)*" (CCRA) or "*Compliant CB*" (SOGIS MRA)..

In accordance with this, Norway recognises Certificates issued under the CCRA and SOGIS MRA.

Norway has achieved status as QP in CCRA, which means the Certificates are internationally recognised.

The remainder of this document describes in more detail how the Scheme is set up, the framework pertaining to security evaluation and certification, and how the actual process is carried out.

2 Principles for the Certification Scheme

The Certification Scheme is grounded in the following principles:

- SERTIT is impartial and unbiased and has no other activities besides its day-to-day tasks involving the Certification Scheme,
- The use of the Certification Scheme is voluntary,
- The basis of the certification is a completed evaluation conducted in accordance with the Scheme's framework conditions,
- The security evaluation is carried out by an approved IT Security Evaluation Facility (ITSEF) that operates according to normal business principles,
- SERTIT approves ITSEFs and oversees their operations,

- The Scheme is not restricted and is available to anyone wishing to apply for certification,
- SERTIT decides whether the product and/or system is suited for certification.

Everyone affected by the Scheme with viewpoints on SERTIT, the Certification Scheme, certification or other matters may provide feedback and input.

3 Organisation and responsibility

The public scheme for certification of IT security is managed by SERTIT.

SERTIT is a part of Norwegian National Security Authority (NSM). The composition of the Certification Scheme is illustrated in appendix¹.

Below is a more detailed description of how the Scheme is organised and what main tasks and areas of responsibility are assigned to the three parts of the Scheme.

3.1 Norwegian National Security Authority (NSM)

NSM is coordinating the preventive safety initiatives and controlling the safety conditions in Norway. The range of responsibility of NSM is partly given by regulations due to the Security Act and partly through the letters of assignment and implementation.

3.2 SERTIT

SERTIT is the public certification authority for IT security.

SERTIT exercises supervisory authority over ITSEFs.

SERTIT's main task as the public certification authority for IT security is to issue Certificates and Certification Reports. SERTIT is also responsible for drawing up rules and framework conditions for the Scheme and for ensuring that the rules are complied with by all parties. SERTIT also oversees the entire evaluation process, which forms the basis for being able to perform certification. SERTIT is also the body that approves commercial evaluation facilities under the Certification Scheme. SERTIT's terms of reference are given in appendix².

To perform the tasks at SERTIT in an appropriate manner, including meeting the formal requirements [5], [6], [17], [18] and [19], so that the Scheme functions efficiently and effectively, its operations are organised in the following manner:

The Head of SERTIT has the overall responsibility for the day-to-day operation of the Scheme. Certification projects are carried out under the supervision of a project manager, who is also responsible for preparing the Certification Report and Certificate. Personnel for this role are designated for individual projects in

¹ Appendix A: Organisation of the Certification Scheme

² Appendix C: Terms of reference for SERTIT

accordance with current procedures specified in the quality system. SERTIT is responsible for the satisfactory performance of tasks pertaining to the quality system, finance/administration, communication and marketing.

The organisation chart of SERTIT is provided in appendix³, which is a graphic presentation of SERTIT and the functions handled in its operations.

3.3 Advisory Board

It is established an Advisory Board for SERTIT that in addition to professional advice shall contribute to necessary communication between the Certification Authority and all parties interested in the Scheme.

3.4 IT Security Evaluation Facilities (ITSEFs)

IT Security Evaluation Facilities (ITSEFs) that carry out assignments for the Certification Scheme are subject to SERTIT's authority. This means that SERTIT is responsible for approving evaluation activities and subsequently performing inspections of the evaluation facility and of all evaluation activities. Evaluation activities are regulated by the provisions of the CCRA [6] and national framework conditions laid down by SERTIT.

The evaluation facilities perform security evaluations of IT products and systems on a commercial basis in accordance with international standards [1], [3], [4], [5] and [17]. ITSEFs perform security evaluations in accordance with defined procedures laid down in a separate quality manual.

Information on approved ITSEFs can be found in Annex A. Updated information on approved evaluation facilities is published at the website sertit.no.

3.5 External parties

A number of external parties are involved in the certification process. Most of these are either sponsors or developers, but other actors may be involved as well. Below are a detailed description of these actors and some guidelines for the certification process.

3.5.1 Sponsors

By *sponsor* is meant an organisation or person who requests a certification for a certain IT product or system. Thus, a sponsor's connection to the IT product or system to be certified may vary.

A sponsor can be a vendor, purchaser, agent acting on assignment from a purchaser, system developer or a consortium representing more than one developer or vendor.

³ Appendix B: Organisation chart of SERTIT – functions and roles

A sponsor can also be the developer of the IT product or system to be certified. Since in many cases developers use subcontractors, the role of developer is described in greater detail in the section below on Developers.

In cases where two or more sponsors are involved, a management group is set up to function as the sponsors' point of contact.

The general framework conditions for the Certification Scheme may place constraints on the contractual relations between the sponsor and the ITSEF.

3.5.2 Developers

By *developer* is meant the company that manufactures the IT product or system to be certified. In cases where a developer does not have the role of sponsor, co-operation between the parties is required in connection with the evaluation process. The developer is responsible for providing ITSEFs with the necessary technical information on the IT product or system. The need for information includes access to the documentation necessary for performing the security evaluation and certification.

In some cases, several developers may be involved in a security evaluation, which may result in problems with gaining access to information crucial to the evaluation. Interactions of this type require the parties to enter into the necessary agreements in advance (see also section 6.8.1).

4 General provisions

This chapter contains some key provisions on Conducting security evaluations, Framework conditions for evaluation activities, Rules for publishing information and Complaints, disputes and responses. For more detailed information, see the publication Sd 003E [20].

4.1 Conducting security evaluations

All engagements for evaluating the security of IT products and systems under the Certification Scheme require the formal prior approval of SERTIT.

The Certification Scheme is based on trust and a neutral professional assessment.

SERTIT oversees that all security evaluations are conducted by an impartial third party and by qualified personnel.

4.2 Framework conditions for evaluation activities

SERTIT lays down the framework conditions for the application process for authorisation as an ITSEF. These include establishment conditions, selection criteria and financial matters.

The purpose of this is to ensure that the Certification Scheme has adequate capacity in relation to market demand and that it functions efficiently and effectively.

The framework conditions for establishing ITSEFs are described in detail in the document [20].

SERTIT will inform the affected parties about changes in the framework conditions.

4.3 Rules for publishing information

The following provisions relating to the publishing of information on SERTIT, the Certification Scheme or certified products apply to users of the Scheme, such as sponsors, developers and ITSEFs:

- The parties must obtain prior approval from SERTIT when issuing press releases or similar information relating to security evaluations and/or certifications under the Scheme,
- The parties may not make statements in press releases, advertising materials or the like which may contain misleading information on security evaluations and/or certifications, or which may damage the Certification Scheme in any manner.

4.4 Complaints, disputes and responses

SERTIT is the body that handles complaints, disputes and responses related to the Certification Scheme. Any individual decision may be appealed pursuant to the Public Administration Act. Complaints or requests by users of the Scheme for changes in a decision made by SERTIT must be submitted in writing to SERTIT. SERTIT will consider the matter and decide whether the decision is to be upheld or not. If a party appeals a decision made by SERTIT, the matter will be brought before the next administrative level, which will determine if the appeal is to be heard.

All conflicts of a technical nature between sponsors, developers or ITSEFs shall be taken up with SERTIT.

5 Financing of the Certification Scheme

The Ministry of Defence is the ministry with budget responsibility and allocates funds to SERTIT through the budget of the Norwegian National Security Authority.

SERTIT's appropriation covers the certification body's annual operating expenses.

6 Preparations for security evaluations

This chapter describes the point of departure for carrying out certification and describes in detail the preparatory phases of the certification process.

The point of departure for initiating a certification process is normally one or more of the following circumstances:

- vendor wants to strengthen its market position,

- system developer is required to satisfy conditions in a specific contract,
- purchaser of a product or system has to comply with the company's own security requirements, industry standards, or statutory security requirements (issued pursuant to law or regulations).

The objective of the preparatory phase is to investigate whether the *Target of Evaluation (TOE)* is clearly defined and whether it is appropriate for certifying.

In addition to TOEs, this includes the following matters: Specification of requirements, the design and quality assurance of the *Security Target (ST)*, identification of the deliverables that are necessary for conducting the evaluation, formal notification of the engagement and the preparation of work plans, the Application for Certification, clarification the purpose and objective of the evaluation.

The individual steps in the preparations are discussed in detail below.

6.1 Specification of requirements

A *Protection Profile (PP)* is a generic set of functional security requirements and requirements for the Evaluation Assurance Level (EAL) for a certain type and/or group of TOE, which has been developed to define the operation's security requirements. Put another way, we may call a PP a specification of security requirements. An ST may consist of all or part of one or more PPs. PPs can be security evaluated and certified in accordance with the requirements of the CC.

6.2 Security target

By *ST* is meant both a specification of the security functions against which a TOE is to be evaluated and a description of the environment in which the TOE is to operate. In other words, an ST is a solution specification.

The sponsor is responsible for designing and assuring the quality of STs. The document is to be submitted to the ITSEF and SERTIT for assessment, who determines whether it is sufficient and appropriate for a security evaluation of the TOE. The sponsor shall be notified in writing of any problems with using the ST submitted before the evaluation starts.

The CC specifies requirements for the form and contents of STs.

Sponsors may use outside assistance for defining STs.

6.3 Deliverables

All matters involving security that are of importance for the security evaluation shall be identified and included in a separate overview. This may include the following:

- TOE (hardware, firmware, software),
- ST,
- documentation (technical, user's and administrator's guide),

- technical assistance from the developer,
- access to the developer's premises,
- access to the operating environment,
- tools.

The deliverables are necessary for carrying out the evaluation. The ITSEF is responsible for documenting the deliverables on a separate list.

6.3.1 Copyright and other rights

It is normally the developer who retains the copyright to the information on the TOE, and the sponsor does not automatically have access to this type of information. This should therefore be regulated in a separate agreement between the parties (see also section 6.8.1, Contractual matters).

6.4 Notification of engagements and the security evaluation work plan

ITSEFs are mandated by SERTIT to notify it of new engagements, "*Task Initiation Notice (TIN)*", and to request its approval for conducting security evaluations under the Scheme. This normally occurs after preliminary investigations of the basis for the security evaluation. The procedures for notifying engagements are defined in separate guidelines for ITSEFs.

A work plan for the security evaluation shall also be prepared and entered on the "*Evaluation Work Plan (EWP)*" form. The EWP is to have a sufficient level of detail that covers all evaluation criteria. The procedures for filling out EWPs are defined in separate guidelines for ITSEFs.

Both documents are to be sent together to SERTIT for detailed assessment, after which a meeting is normally held between the parties.

On the basis of the formal request from the ITSEF, the Head of SERTIT designates authorised personnel to oversee the activity from then on.

6.5 Application for certification

The sponsor is responsible for applying to SERTIT for certification. A separate application form [21] has been prepared, which can be downloaded from SERTIT's website and shall be used in all formal enquiries relating to certification.

The application form contains instructions for completing it and provides detailed rules for awarding and using the Certificate. The application obliges the sponsor to follow all the rules in the Certification Scheme, and not to subject the Scheme to unlawful or undesirable conditions or otherwise do damage to the Scheme.

To ensure an efficient certification process, it is recommended that the application with necessary attachments is sent to SERTIT simultaneously with the ITSEF's submission of the Task Initiation Notice (TIN) and the EWP, since the application cannot be processed before the TIN and EWP have been submitted.

6.6 Clarifications and commitments

Before binding agreements for a security evaluation and subsequent certification are signed, it is important for the sponsor to investigate the case together with SERTIT, including whether the proposed TOE can, in principle, be certified under the Scheme. In practice this normally takes place when the sponsor, the ITSEF and SERTIT discuss the case at a start up meeting. The start up meeting usually takes place after the parties have assessed the existing documentation, provided that there is a high probability for being able to carry out certification.

One purpose of the meeting is to ensure that the parties involved are sufficiently familiar with the TOE and have a common understanding of the certification process.

6.7 Approval of the certification engagement

SERTIT may grant an application to conduct a security evaluation and certification if there is a fundamental basis for this being implemented within the framework of the Scheme. This means that the following requirements must be satisfied:

- Certification must be appropriate,
- The formal requirements for certification must be met,
- The security evaluation and certification must be able to be implemented in an impartial manner,
- The security evaluation and the Certification Scheme must be in conformance with international and national regulations,
- According to the EWP, all obligatory evaluation activities must be planned and the plans must reflect a realistic time frame. The plans must contain sufficient resources, including quantities, competence and necessary equipment,
- There must be a high level of probability that all evaluation activities can be carried out as planned,
- Any other factors that indicate that certification cannot be carried out.

Although approval may be granted orally at a meeting with the parties, it must subsequently be confirmed by a formal approval. A confirmation shall be given that the ST, TOE, deliverables and EWP can be accepted as part of the proposed security evaluation under the Certification Scheme. The approval will be sent to all parties involved.

6.8 Use of consultants

The use of consultative assistance for the preparation of a security evaluation is not subject to SERTIT's control and is therefore subject to negotiations between the sponsor and the ITSEF or other consultants. The use of consultants for development or preparations for an evaluation is normally unproblematic as long as the facility can show that the requirements for impartiality are being met. The ITSEF should therefore be scrupulous in defining the level of its involvement in solving the

problem to ensure that the facility's independent status is not compromised and does not later prevent an impartial security evaluation.

SERTIT recommends that the parties sign an agreement that regulates all matters connected with the use of consultants, *inter alia* to ensure that the necessary degree of impartiality is maintained.

In the event of any doubt of impartiality in the case, the ITSEF shall contact SERTIT for confirmation that there are no objections to performing the job as specified.

SERTIT decides whether the ITSEF is qualified to carry out a security evaluation under the Certification Scheme. The decision will partly be based on the ITSEF's involvement in the consultancy activities and its capacity to sustain the necessary impartiality. It is mandatory for the ITSEF to notify SERTIT of all consultancy activities related to the evaluation engagement.

6.8.1 Contractual matters

The sponsor is urged to solicit tenders from several ITSEFs in connection with preparing or carrying out a security evaluation.

ITSEFs are mandated by SERTIT to enter into an agreement with the sponsor in connection with engagements for security evaluation under the Certification Scheme. Such a binding agreement should exist in advance of evaluation activities. Although it is up to the parties to specify the details of such agreements, the following factors ought to be included:

Specifying the need to obtain access to previous evaluation reports wanted by the sponsor,

The agreement should deal with all matters related to Deliverables, as specified in section 6.3. This includes timetables for procuring deliverables, right of access to information and requirements for storage. The ownership rights to information should be clarified before the engagement starts.

All matters relating to enterprise-sensitive information should be dealt with in the agreement.

SERTIT recommends that the agreement regulate all matters connected with the use of consultants, to ensure that the necessary degree of impartiality is maintained. This also applies in cases where consultancy engagements are undertaken outside the framework of the Certification Scheme, but which are related to products/systems that subsequently are the subject of security evaluation and certification.

It is the sponsor's responsibility to obtain the written permission from the developer to gain access to enterprise-sensitive information as well as to relinquish its own rights to evaluation results that may compromise such information.

The sponsor may not simply withdraw from a certification assignment once it has begun. SERTIT requires in general that the ITSEF has regulated all matters relating to any breach of contract in a separate agreement for each engagement. Duties with lack of progress for 6 months may be terminated.

7 Security evaluation

This chapter describes the main features of the implementation of a security evaluation and the collaboration among the parties in the process. The chapter also describes the steps that go into the preparation of the *Evaluation Technical Report* (ETR).

7.1 Objectives

By *security evaluation* is meant in this context judging whether an IT product or system meets the requirements of the ST. This covers such things as assessing a detailed evaluation of the TOE to establish how well it meets the ST as well as identifying possible faults and shortcomings. The objective is to enable the ITSEF to prepare an unbiased report which establishes whether or not the TOE meets the ST.

7.2 Implementation

The technical security evaluation of the TOE and deliverables is carried out in accordance with the approved EWP. The security evaluation is conducted in accordance with current international regulations through the CCRA, SOGIS MRA, CC, CEM and other national framework conditions laid down by SERTIT.

Any changes to the EWP shall be assessed and approved by SERTIT, to ensure that the proposed work is adequate, that the plans are realistic and that the necessary resources are available. Besides the decisions made in last sentence in ch. 6.8.1, Contractual matters, should be pointed out.

Both SERTIT and the ITSEF must take care that the integrity of the security evaluation is not compromised. By this is meant that the developer shall not have the opportunity to influence the results or prevent an accurate and fair presentation of the results of the security evaluation.

7.2.1 Observation reports and journal

If faults and shortcomings are uncovered in the TOE during the security evaluation, this is to be noted in an *Evaluation Observation Report (EOR)*. The EOR shall then be communicated to the sponsor and SERTIT for further consideration.

The sponsor shall respond to the EOR in writing with detailed recommendations for correcting proven faults and shortcomings as well as a timetable for any corrections. The corrections may require adjustments in the deliverables and may have consequences for the EWP. Viewpoints from SERTIT are normally sent on a special review form. The EOR and comments on the EOR are case documents for the progress meetings (see section 7.2.2.). The process normally proceeds in iterations between the parties until the EOR problem is resolved. In instances where it is impossible to resolve an EOR problem, please refer to the penultimate paragraph in section 7.2.2, Interaction.

In addition to the EOR, the ITSEF shall document on an ongoing basis the results of the security evaluation in a separate log for each evaluation engagement. SERTIT may examine the log when necessary.

7.2.2 Interaction

Progress meetings for the security evaluation are held between the ITSEF and sponsor. SERTIT convenes and chairs these progress meetings. Besides SERTIT, the ITSEF, developer and sponsor shall attend. The EWP shall indicate the schedule for the progress meetings.

The ITSEF normally needs to communicate directly with the developer concerning the TOE, deliverables or other matters. Thus, the ITSEF is required to have concluded the necessary agreements with the sponsor concerning such communication.

Discussion of the EOR is a key part of progress meetings. Proposals for resolving problems from the sponsor are discussed by the parties with a view to finding acceptable solutions at the earliest possible stage in the evaluation process. If necessary, an EOR problem can be resolved at the meeting, in which case the conclusion shall be included in the minutes.

If it is not possible to correct the faults or shortcomings, and this will have consequences for the outcome of the certification process, SERTIT shall notify the sponsor of the consequences. The sponsor may then choose to:

- terminate the security evaluation,
- continue the security evaluation and accept the problems and consequences for the evaluation, for example by adopting a lower Evaluation Assurance Level (EAL),
- modify the evaluation plan and, in consultation with SERTIT, instruct the developer to make the necessary changes in the TOE.

The sponsor must confirm in writing the chosen alternative.

7.2.3 Inspection

As part of its oversight activities, SERTIT may perform the inspections necessary to ensure that the framework conditions for the security evaluation are followed. SERTIT may be present during testing.

SERTIT reserves the right to attest to security evaluations on terms to be specified in detail between the parties.

7.3 Evaluation Technical Report

All security evaluation findings are to be documented in the Evaluation Technical Report (ETR). This report shall be prepared according to current guidelines on a template provided by SERTIT. The framework is based on the requirements given by CCRA, Annex I and CC/CEM. The ETR constitutes the end product of the ITSEF's work, and forms the basis for the *Certification Report (CR)*.

The conclusions of the ETR are to establish which parts of the evaluation criteria have or have not been met, while providing sufficient evidence for this.

7.3.1 Protection of information and protection marking of the ETR

It must be clearly stated in the report that the contents are to be regarded as company-internal information and must not be made public. If the contents do not fall under the Security Act or other national provisions, the ETR must be clearly marked as being information for internal use only.

As regards the protection of sensitive information in connection with security evaluations and evaluation reports for systems in undertakings subject to the Security Act or corresponding provisions, all information shall be marked as protected in accordance with the provisions in force at the time in question.

The developer may request or require limiting the sponsor's access to company-sensitive information. SERTIT and the ITSEF are to ensure that the sponsor does not obtain access to information of this kind. The ITSEF is responsible for the scope of this type of information being clearly defined and the rules for protecting such information being obeyed.

7.3.2 Release of the ETR

If the developer has requested that company-internal information is not to be disclosed to the sponsor, the ITSEF is to make sure that the ETR does not contain this kind of information before releasing the report. The ITSEF normally addresses this concern by preparing a short version of the ETR, which is then released to the sponsor for review. It should appear on the document whether it is preliminary or final, or whether it has been approved by the certification body.

SERTIT may refuse to carry out certification, if the developer without due cause withholds necessary company-internal information.

7.3.3 Assessment and approval of the ETR

SERTIT reviews the ETR with supporting documents and examines whether the security evaluation has been conducted in accordance with the agreed criteria, methods and procedures in the Scheme and whether the ETR provides sufficient basis for preparing the Certification Report (CR).

For the ETR to be approved, all comments must be addressed and the evidence must be sufficient and consistent pursuant to CCRA and CC/CEM requirements.

SERTIT then issues a confirmation that the security evaluation is completed and at the same time informs the parties concerned when the CR is ready to be made public.

8 Certification

This chapter provides a top-level description of the certification process and explains the purpose of the Certification Report (CR) and the Certificate.

The certification process concludes with a formal confirmation of the evaluation results and of whether the evaluation criteria, methods and procedures have been correctly applied. Plans for providing maintenance of the Certificate are described in more detail in Chapter 9.

8.1 The certification process

The certification process begins when there is an approved ETR. As needed, SERTIT may ask the ITSEF for access to particular technical evidence and results to support the conclusions stated in the ETR. At the same time, other documents from the security evaluation, observations from testing and results from other supervisory activities constitute important material on which the certification may be based. Sections 8.2 and 8.3 provide a more detailed description of the Certification Report and the Certificate, respectively.

8.2 Certification Report

SERTIT shall document all findings from the evaluation in a Certification Report. The purpose of the Certification Report is to confirm whether the TOE is in compliance with the ST and to identify any vulnerabilities that could be exploited. The Certification Report confirms the Evaluation Assurance Level (EAL) that has been attained. The Certification Report can recommend suitable countermeasures to neutralise any vulnerabilities. The Certification Report confirms that the security evaluation has been conducted in accordance with the framework conditions of the Scheme and that the conclusions are consistent and in line with the evidence submitted.

However, the Certification Report provides no guarantee that all faults and shortcomings in the TOE have been revealed. But the likelihood of undetected faults or shortcomings becomes lower the higher the EAL on which the evaluation is based.

8.3 Certificate

When the Certification Report is finalized, a Certificate may be issued. The Certification Report shall be attached to the Certificate. The Head of SERTIT gives the final approval of the Certificate and Certification Report.

The issuance of a Certificate does not imply any form of recommendation by SERTIT of the TOE concerned. The Certificate is valid only for the version, platform and environment under which the TOE was evaluated. The sponsor may market a product as certified only when holding a valid Certificate. SERTIT may require that the sponsor provide reference material or documentation that clearly indicates the correct version of the TOE.

8.3.1 Rights

SERTIT holds the copyright on the Certification Report and the Certificate. Reproduction and distribution is permitted provided that the Certification Report is copied in its entirety.

8.3.2 Certified products

SERTIT will regularly publish an overview of products certified under the Scheme. The information will be published on SERTIT's website. Enquiries relating to certification, the Certification Scheme or other matters may be directed to SERTIT.

8.3.3 Use of Certificates

The following provisions apply to the use of the Certificate:

- The Certificate may be used only in connection with the product/system to which the Certificate applies,
- The Certificate may be used only to document the product's/system's compliance with the standards on which SERTIT bases its activities,
- The certification must not be used in an erroneous or misleading manner that brings or may bring SERTIT or the Certification Scheme into disrepute,
- The certification may not be used in advertising or marketing if the Certificate is revoked or withdrawn,
- The vendor is obliged to have implemented registration and handling of complaints regarding certified products and made these registrations available to SERTIT.

The vendor is obliged to notify SERTIT of any changes to factors that were the object of the security evaluation of the certified product.

8.3.4 Monitoring Certificates

Monitoring Certificates primarily takes place through a review of information from the sponsor. Statements about certified products in advertising, the media or on the sponsor's website or other matters coming to SERTIT's attention may be made the subject of further investigation. The purpose of this monitoring is to see to it that the Certificates are used in accordance with the provisions stated in section 8.3.3, Use of Certificates. Certificates are monitored in accordance with defined procedures.

8.3.5 Sanctions in the event Certificates are misused

If Certificates are misused, SERTIT may initiate sanctions pursuant to ISO/IEC Guide 27 [13]. Sanctions are implemented in accordance with defined procedures. The two most common corrective actions are:

- Request for withdrawal of the Certificate,
- Removing the certification mark from the product.

9 Maintenance of the Certificate

A Certificate is valid only for a specific version of a TOE. However, most TOEs undergo changes at a later point of time. These changes are not a part of the scope of the certification. With future changes to a TOE, there is a need for an end-user to have the same degree of confidence in the new version of the TOE as in the original certified version. Therefore the CCRA established framework conditions for maintenance of Certificates, ref. [1]. Questions related to Certificate Maintenance in SERTIT are addressed in compliance with this framework.

The TOE can, in some circumstances, be part of the Certificate Maintenance programme. The framework conditions are called "Assurance Continuity", and can be downloaded from the CCRA website (www.commoncriteriaportal.org). For more information of the Maintenance programme, please contact SERTIT.

10 Abbreviations

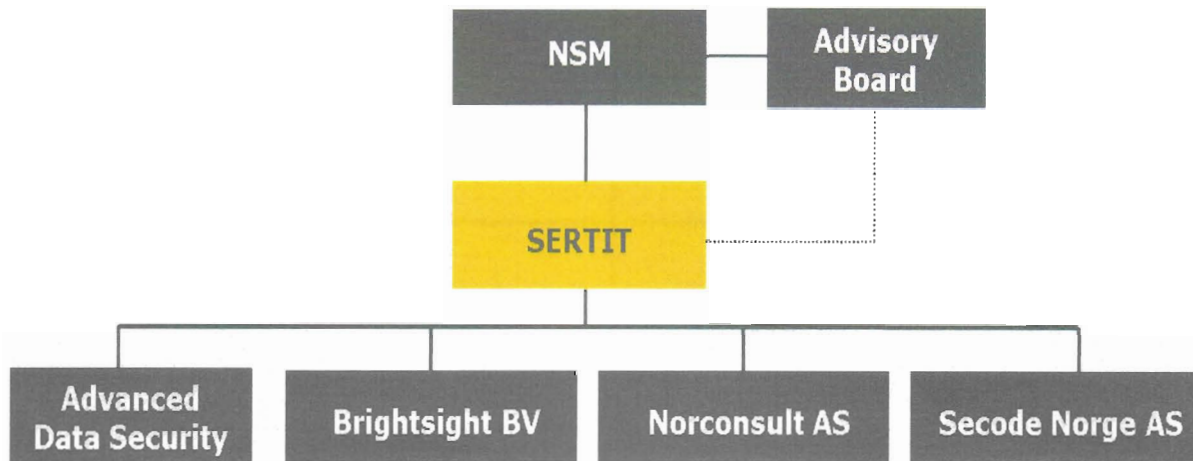
CC	Common Criteria
CCRA	Arrangement on the Recognition of the Common Criteria Certificates in the field of Information Technology Security
CEM	Common Evaluation Methodology for Information Technology Security
CR	Certification Report
EAL	Evaluation Assurance Level
EOR	Evaluation Observation Report
ETR	Evaluation Technical Report
EWP	Evaluation Work Plan
ITSEF	IT Security Evaluation Facility (approved under the Norwegian Certification Scheme)
NSM	Norwegian National Security Authority
PP	Protection Profile
QP	Qualified Participant
SERTIT	Norwegian Certification Authority for IT Security
SOGIS MRA	SOGIS Mutual Recognition Agreement
ST	Security Target
TIN	Task Initiation Notice
TOE	Target of Evaluation

11 References

- [1] CCIMB-2004-02-009, Assurance Continuity: CCRA Requirements, version 1.0, February 2004.
- [2] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Current version.
- [3] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, Current version.
- [4] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, Current version.
- [5] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, Current version.
- [6] CCRA, "Arrangement on the Recognition of the Common Criteria Certificates in the field of Information Technology Security", 23 May 2000.
- [7] Common Evaluation Methodology for Information Technology Security, Part 1: Introduction and general model, Current version.
- [8] FOR-2012-06-22-653, Regulation of 1 July 2012, journal no. 2012-0576 relating to information security, Ministry of Defence, cf. Royal Decree No. 721 of 29 June 2001.
- [9] FOR-2012-06-22-641, Regulations of 1 July 2012, journal no. 2012-0575 relating to security classified procurements, Ministry of Defence, cf. Royal Decree No. 721 of 29 June 2001.
- [10] FOR-1998-12-11-1193, Regulation No. 1193 of 11 December 1993 relating to public archives, 1 January 1999, Ministry of Culture and Church Affairs.
- [11] FOR-2007-04-24-442, Regulation of 4 July 2007 relating to supplemental technical and archive-related provisions relating to the management of public archives, 1 January 2000, Ministry of Culture and Church Affairs.
- [12] FOR-1972-03-17-3352, Regulation No. 3352 of 17 March 1972, Instructions for handling of documents in need of protection for reasons other than those mentioned in the Security Act with regulations (the Protection Instructions)
- [13] ISO/IEC Guide 27:1983, "Guidelines for corrective action to be taken by a certification body in the event of misuse of its mark of conformity"
- [14] Act of 10 February 1967 relating to procedure in cases related to the public administration (Public Administration Act), Ministry of Justice and the Police.
- [15] Act No. 31 of 14 April 2000 relating to the processing of personal data (Personal Data Act), Ministry of Justice and the Police.

- [16] Act No. 10 of 20 March 1998 relating to protective security services (Security Act), 18 April 1997, Ministry of Defence.
- [17] NS-EN ISO/IEC 17025, General requirements for the competence of testing and calibration laboratories, Norwegian Standards Association (NSF), 1999.
- [18] NS-EN 45011, General requirements for bodies with systems for product certification (ISO/IEC Guide 65), 2nd Edition, 1998, Norwegian Standards Association (NSF).
- [19] NS-EN ISO/IEC 17065:2012, Conformity assessment Requirements for bodies certifying products, processes and services (ISO/IEC 17065:2012), September 2012, Standard Norge.
- [20] Sd 003E, Requirements regarding IT Security Evaluation Facilities, Current version, SERTIT.
- [21] Sd 027E, Application for certification, v. 1.0, 16 September 2004, SERTIT.
- [22] Certification of IT security in products, systems and organisations (final report), 13 November 1997, Norwegian Council for IT Security. (In Norwegian only)
- [23] SOGIS MRA, Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, Version 3,0, January 8th 2010.

Appendix A: Organisation of the Certification Scheme

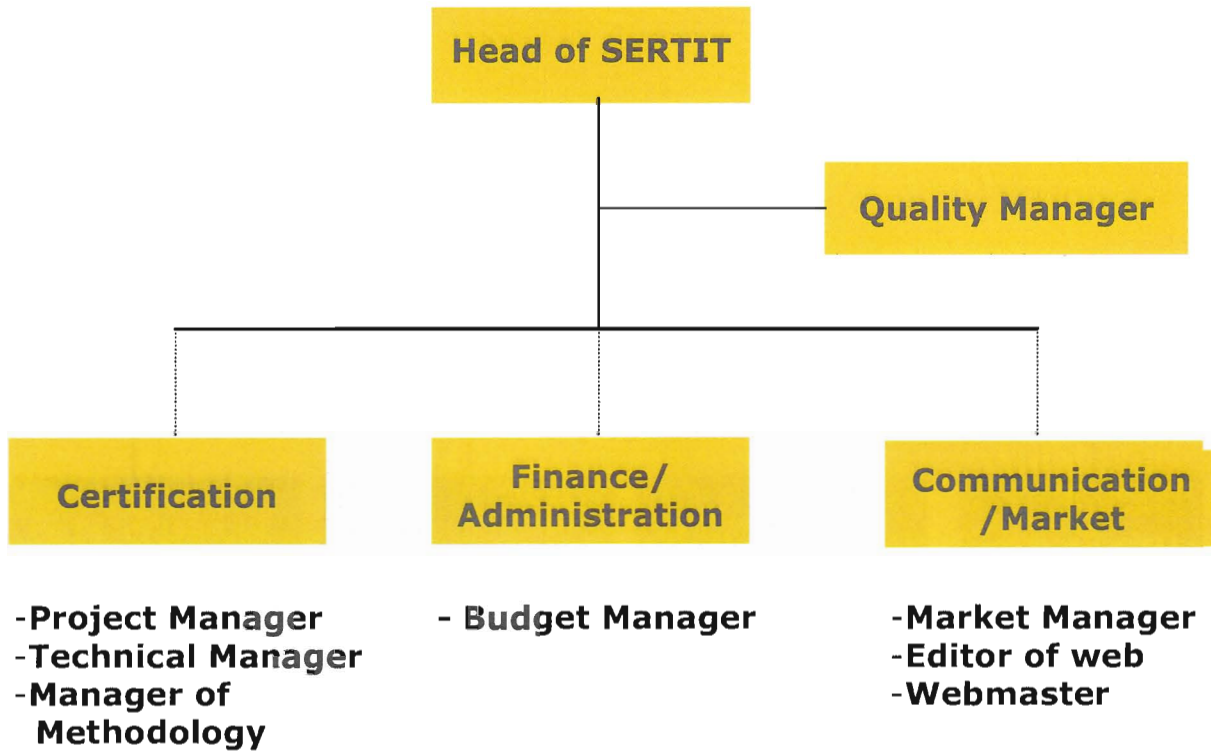


SERTIT exercises oversight responsibility over four approved commercial evaluation bodies: Advanced Data Security, Brightsight BV, Norconsult AS and Secode Norge AS. SERTIT draw up framework conditions for IT Security Certification in Norway, and issues Certification Reports and Certificates based on security evaluations conducted by the evaluation facilities.

SERTIT has been placed under the Norwegian National Security Authority (NSM), and SERTIT's activities are organised as a part of this directorate. NSM is coordinating the preventive safety initiatives and controlling the safety conditions in Norway. The range of responsibility of NSM is partly given by regulations due to the Security Act and partly through the letters of assignment and implementation.

The Head of SERTIT reports to the head of the Communication and Security Department in NSM.

Appendix B: Organisation chart of SERTIT – functions and roles



The Head of SERTIT is responsible for the day-to-day management of the Scheme and has certification authority. SERTIT is staffed with 3.5 full-time equivalents (FTEs). SERTIT's activities are arranged in line with the requirements defined in NS-EN 45011 [18], and a person has been designated with responsibility for the quality system. The person in question is responsible for ensuring that a quality system is established, implemented and maintained. Oversight of ITSEFs is also covered by the quality system. The quality manager reports to the Head of SERTIT.

Certification activities in the individual projects are handled whereby a responsible project owner is designated in accordance with the criteria and procedures stipulated. The person in question is *inter alia* responsible for supervising the security evaluation and preparing the Certification Report and Certificate. The project owner reports to the Head of SERTIT. It is the Head of SERTIT who gives the final approval of the security evaluation and the result of certification.

The remaining tasks in the organisation in finance/administration and communication/marketing are performed in part internally at SERTIT or at NSM. These other functions report to the Head of SERTIT.

Appendix C: Terms of reference for SERTIT

For further information on the authorisation of SERTIT's operation and the basis of the Scheme, please refer to documents from the Ministry of Trade and Industry of 1 February 1999 and 14 April 1999 both ref. 98/4561-F-IKT eja/lem in the quality system's document list.

1. The public IT Security Certification Authority, SERTIT is organised as a part of the Norwegian National Security Authority. The activities are managed by dialog rule with the Ministry of Defence (FD) and the Ministry of Justice and Public Security (JD).
2. To meet the needs of the public and private sectors, SERTIT shall perform the following tasks:

Administrative tasks


- a. Function as the secretariat for the Advisory Board,
- b. Prepare budgets and manage financial affairs,
- c. Register for certification all evaluations under the Scheme,
- d. Keep an overview of the professional status of the employees of IT Security Evaluation Facilities,
- e. Issue Certificates for products and systems,

External tasks

- f. Provide information on the Scheme,
- g. Approve press releases and similar statements concerning the Scheme,
- h. Document and publish a description of organisational structure, framework conditions and procedures of the Scheme and provide for necessary updating,

Professional tasks

- i. Authorise IT Security Evaluation Facilities (ITSEFs),
- j. Supervise the authorised evaluation bodies, oversee their work and how it is performed, their compliance with the provisions of the Scheme and their capacity to achieve the objectives of the Scheme,
- k. Ensure that all procedures and routines followed by IT Security Evaluation Facilities (ITSEFs) comply with the provisions of the CCRA and ensure that sensitive information concerning products, systems and protection profiles (and solution specifications) in the evaluations are managed and protected in accordance with requirements and that these routines are followed,
- l. Develop and maintain a Norwegian evaluation methodology and ensure consistency with the international criteria and methods existing at any given time,

- 
- m. Provide guidance, support and standards for training for evaluation bodies,
 - n. Verify the appropriateness of the basis for evaluation of products and systems, approve evaluation work plans and issue lists of what shall be produced and delivered in connection with certification,
 - o. Prepare a Certification Report for each completed and approved evaluation,
 - p. Confirm the evaluation result under the Scheme and provide details of certified and registered products in a separate list of certified products,

International tasks

- q. Establish connections with national and international bodies regarding mutual recognition of Certificates,
- r. Represent Norway in the CCRA and SOGIS MRA as obliged through the arrangement and the agreement respectively.