



International Systems Security Engineering Association



*International Certification Program -
Systems Security Engineering-
Capability Maturity Model (SSE-
CMM/ISO/IEC* Standard 21827)
Appraiser*

January 27, 2006



Table of Contents

Certification Body	4
Organizational Structure	5
Certification Scheme	6
Management System	6
Outsourcing for SSE-CMM Appraisal Methodology Training	7
Third-Party Providers of the SSE-CMM Appraisal Methodology Training	7
Certification Records.....	9
Confidentiality	10
Certification Body Personnel Requirements	10
Examinations	11
Requirements for the Administration of the Examination	12
Examination Proctor Requirements.....	12
Impartial Examination Validation/Grading Process	13
Certification Process	13
Application	13
Evaluation.....	14
Required Documentation	14
Certification Decisions.....	14
Re-Certification.....	15
Certificates.....	15
Appeals and Complaints	15
SSE-CMM Appraiser Certification Requirements	16
1. SSE-CMM Entry-Level Appraiser –	16
2. SSE-CMM Appraiser –	17



3. SSE-CMM Lead Appraiser –	19
Recertification	20
Grandfathering Requirements for the SSE-CMM Appraiser or SSE-CMM Lead Appraiser	20
Exceptions	22
Control of Non-Conforming Activities	22
Fee Structure	22
ISSEA Membership	22
References	23
Definitions	23
Appendix A: Code of Ethics	24
Appendix B: SSE-CMM Appraiser Examination Registration Form and Application for Certification	26
Appendix C: Application for Review and Approval of Third-Party SSE-CMM Training and/or Authority to Administer the SSE-CMM Appraiser Exam	28



*General Requirements for Certification in
Systems Security Engineering and the
Systems Security Engineering- Capability
Maturity Model (ISO/IEC Standard
21827:2002 SSE-CMM)) Appraisal
Methodology*

Certification Body

The Certification Body has been developed and will be administered under the auspices of the International Systems Security Engineering Association (ISSEA), which functions per industry competitive selection and ISO recognition as the Systems Security Engineering –Capability Maturity Model Sustaining Organization (SSO). ISSEA will manage the SSE–CMM appraisal certification process and the SSE professional certifications in accordance with Reference 1 and its charter as the SSO. Certification under this program is available without discrimination to all who meet the requirements described herein.

Under its charter as the SSO, the certification body meets the following criteria as defined in ISO/IEC 17024, General Requirements For Bodies Operating Certification Schemes For Persons:

1. The policies and procedures of the certification body and their administration are non-discriminatory, and comply with all applicable regulations and statutory requirements. The certification body does not use procedures to impede or inhibit access by applicants and candidates except as provided for in this standard.
2. The certification body, henceforth referred to as ISSEA, has responsibility for defining the policies for granting, maintaining, renewing, expanding, suspending and withdrawing certification.
3. ISSEA confines its requirements, evaluation, and decisions on certification to those matters related specifically to the scope of the desired certification(s).
4. ISSEA has the responsibility for defining the uniform competence requirements on the basis of ISO 21827, Systems Security Engineering – Capability Maturity Model (SSE-CMM), and the requirements and procedures for the evaluation of certification candidates (including monitoring and re-certification). ISSEA will ensure that updates of these requirements are in line with developments in technology and process definitions.



5. ISSEA is responsible for defining a process for the development of the certification scheme and provide due notice to interested parties of any changes in certification requirements.

Organizational Structure

ISSEA as the certification body is structured in such a manner as to give confidence to certification candidates in its competency, impartiality, and integrity.

In particular, the certification body (ISSEA) is:

1. Independent and impartial in relation to applicants, candidates, and certified persons, including employers and customers, and takes all possible steps to ensure ethical operations.
2. Responsible for its decisions relating to the granting, maintaining, renewing, expanding, reducing the scope, suspending and withdrawing of certifications.
3. Comprised of a management and committee structure that is responsible for:
 - a. Qualification, evaluation, certification and monitoring of certification in accordance with applicable standards.
 - b. Formulation of policies in relation to the operation of ISSEA as a certification body.
 - c. Decisions on certification.
 - d. Implementation of policies and procedures.
 - e. Finances of the certification body.
 - f. Delegation of authority to the certification working group to undertake defined activities on its behalf.
4. In possession of documentation establishing it as a legal entity.

ISSEA has a structure, which ensures impartiality. A certification working group (committee) has been established to work on behalf of ISSEA to develop and maintain the certification scheme for each level/type of certification under consideration. The committee represents the interests of the profession, without any particular industry predominating.

In the execution of its charter as the certification body, ISSEA shall:

1. Ensure that individuals other than those executing the certification evaluations undertake certification decisions.



2. Have access to the financial resources essential to establish and operation the certification process.
3. Have policies and procedures, which distinguish between the certification of persons and other activities.
4. Ensure that the activities of related bodies and organizations do not compromise the confidentiality, impartiality, and integrity of the certification process.
5. Ensure that assistance is not provided to other agencies to prepare training services that compromise the confidentiality, impartiality, and integrity of the certification process.
6. Provide or sponsor training, and ensure that the separation of training and evaluation of candidates is managed to ensure the confidentiality, impartiality, and integrity of the certification process.
7. Define policies and procedures for the resolution of appeals, complaints, or disputes from applicants, candidates, and certified persons, their employers and others parties concerned about the certification process, qualification criteria, as well as policies and procedures for the performance of certified persons.
8. Ensure the availability of sufficient staff with the necessary education, training, technical knowledge, and experience to perform certification functions related to the type, range and volume of work performed, as well as a responsible management structure.

Certification Scheme

Management System

ISSEA, as the certifying body, is responsible for defining and documenting its quality policy, including quality objectives and commitment. In executing this function, ISSEA will establish and maintain a documented management system using the concepts of ISO 9001.

ISSEA has designated an individual with direct access to management with the authority to:

1. Ensure that a standardized management system is established and maintained in accordance with the international standard and this document.
2. Report on the performance of the certification management system to organizational management levels.



3. Manage an audit and internal review process focused on continual improvement, corrective and preventive actions.

Outsourcing for SSE-CMM Appraisal Methodology Training

ISSEA may directly outsource work related to certification (training development, training presentation, and proctoring of the approved certification examinations) to an external body. In this case, a properly documented agreement will be drawn up covering the arrangement, confidentiality, and prevention of any conflict of interest. Certification decisions will not be outsourced.

ISSEA as the outsourcing body will:

1. Ensure and take full responsibility for the correctness and appropriateness of the knowledge content and the quality of training by outsourced external body/sub-contractor and will maintain its responsibility for granting, maintaining, renewing, expanding, reducing the scope, withdrawing, and suspending certification.
2. Ensure that the subcontractor is competent and complies with the applicable provisions and is not involved, either directly or through their employer, with training or the maintenance of the competence of persons in such a way that impartiality could be compromised.

Third-Party Providers of the SSE-CMM Appraisal Methodology Training

ISSEA may review and approve SSE-CMM training courses developed for presentation by third-party providers. In order to ensure the consistency and quality of the SSE-CMM appraiser training, ISSEA has implemented a program for approval of third-party SSE-CMM training courses. Third-party providers of training will not be authorized to make certification decisions.

ISSEA will maintain the SSE-CMM Certification Working Group as the reviewing and approving body of third-party providers. As such, the Working Group shall ensure that all independently developed training meets the quality and content requirements of the SSE-CMM Certification program as defined by ISSEA.

ISSEA shall maintain a list of suppliers of approved training courses on the ISSEA web site and documented procedures for assessing and monitoring competence and performance of outsourced work.



In order to meet the requirements for review and approval by ISSEA, appropriate training must:

- Cover the subject matter in satisfactory depth;
- Be effectively presented;
- Provide sufficient means to measure the student's comprehension and performance.

Determining whether a given training course meets the essential criteria requires a rigorous process for evaluating and approving training courses. The ISSEA process for the SSE-CMM Certification Working Group to follow when approving training course providers offers the assurance that the appraisers who successfully complete the ISSEA reviewed and approved courses have been properly trained to conduct system security appraisals.

The course review and approval process includes:

- Review and approval of the course content and the instructors by resume; and
- Evaluation of the course provider's administration system based on written submission of the administrative processes implemented by the course provider.

If formally requested and authorized by the training provider, ISSEA-reviewed and approved courses and trainers will be posted to the ISSEA web site. Any significant modifications to the approved courseware will necessitate resubmission to the SSE-CMM Certification Working Group and ISSEA for review and approval as a prerequisite to retaining approval status.

ISSEA does not reserve the right to deny the development and presentation of SSE-CMM appraisal training offerings by third party organizations.

However, as the appraiser certifying body, ISSEA does reserve the right to review course materials and instructor credentials for third-party organizations requesting the authorization to administer the ISSEA-approved examinations for the SSE-CMM appraiser certificate.

The official ISSEA SSE-CMM appraiser and professional examinations may only be administered either by an ISSEA-outsourced training organization, an ISSEA reviewed and approved training organization, or by a third-party organization in accordance with the requirements of ISSEA examination proctoring procedures. The authorization to administer the SSE-CMM must be formally requested together with a description of the administrative procedures to be followed to ensure the integrity of the examination process.

Approved training organizations may allow the participation in the examination of candidates from other course providers or candidates who



elect to re-take the examination subsequent to unsuccessful prior examination efforts.

Certification Records

ISSEA, as the certification body, shall maintain a system of records, or a registry of certifications, that demonstrate that certification requirements have been effectively fulfilled, particularly with respect to application forms, evaluation reports, surveillance activities and other documents relating to granting, maintaining, renewing, expanding, reducing, suspending and withdrawing certification.

The system of individual certification records to be employed by ISSEA will include the following information:

1. Name of certification candidate
2. Employer
3. Contact Data (Address, Phone Numbers, Email)
4. Certification Status (Level, Date of Certification)
5. Related Prior Experience
6. Related Prior Education
7. Pending Certifications
8. Continuing Education Units (CEUs) relevant to certification status (maintenance, advanced certification, etc.)

With specific applicant permission, information maybe placed on the web site in such a manner to enable public access. Only those data elements explicitly authorized by the data owner will be available on the web site, but may include:

1. Name
2. Employer
3. Contact Information
4. Certification Status

ISSEA shall identify, manage and dispose of records in such a way as to ensure the integrity of the process and the confidentiality of the information. Individuals within the ISSEA record system may have access to their records at any time upon request, which may be submitted in written or oral format. Proof of identity may be required prior to release of the information.



ISSEA will not provide personally identifiable information to third parties without the explicit permission of the data owner.

The records shall be kept for an appropriate period of time to demonstrate continued confidence for at least one full certification cycle, or as required by recognition arrangements, contractual, legal or other obligations.

Confidentiality

ISSEA shall have adequate arrangements consistent with applicable regulations and statutory requirements (laws) to safeguard confidentiality of the information obtained in the course of its certification activities at all levels of its organization, including committees and external bodies (outsourcing) or individuals acting on its behalf.

Information gained by ISSEA in the course of certification activities about a particular applicant, candidate or certified person shall not be disclosed to a third party without the written consent of the respective person. When the certification body is required by regulations and statutory requirements to release information to a third party, the applicant, candidate or certified person shall be informed in advance what information has been requested.

Certification Body Personnel Requirements

In order to ensure that the certification process is carried out effectively and uniformly, the competence requirements for personnel involved in the entire process have been defined by the certification body and reviewed by the responsible certification working group committee and the Sustaining Members Board of ISSEA as the certifying body.

In this context:

1. ISSEA requires its personnel (internal or external) associated with the certification process to sign a document (Attached) by which they commit themselves to comply with the rules defined by the certification body, including those relating to confidentiality and those relating to independence from commercial and other interests, and from any prior and/or present link with the persons to be examined that would compromise impartiality.
2. ISSEA has established clearly documented instructions (Attached) that are available to the personnel describing their duties and responsibilities. ISSEA will ensure these instructions shall be kept current.
3. All ISSEA or related personnel involved in the certification decision activities will possess appropriate educational qualifications, experience and technical expertise, which satisfies defined competence criteria for the tasks identified. As required, ISSEA



shall train selected individuals for their specific responsibilities within the certification body and ensure these individuals are made aware of the significance of the certification offered.

ISSEA will establish and maintain current documentation on the relevant qualifications of the individuals involved in the certification process. The information is accessible to the individuals concerned and includes:

1. Name and address;
2. Organization affiliation and position held;
3. Educational qualification and professional status;
4. Experience and training in the relevant field of the certification body's competence;
5. Their specific responsibilities and obligations within the certification body;
6. Performance appraisals within the certification process; and
7. Date of most recent updating of records.

ISSEA shall identify, manage and dispose of records of the Certification Body Personnel in such a way as to ensure the integrity of the process and the confidentiality of the information. Individuals within the ISSEA Certification Body Personnel record system may have access to their records at any time upon request, which may be submitted in written or oral format. Proof of identity may be required prior to release of the information.

ISSEA will not provide personally identifiable information to third parties without the explicit permission of the data owner.

The records shall be kept for an appropriate period of time to demonstrate continued confidence for at least one full certification cycle, or as required by recognition arrangements, contractual, legal or other obligations.

Examinations

Examinations are considered an essential part of the evaluation for each type and level of certification. ISSEA shall manage the preparation of and approve all examinations to ensure that they are planned and structured in a manner which ensures that all appropriate competence criteria are objectively and systematically evaluated with sufficient information/evidence (records) produced to confirm competence. Only those examinations directly developed and provided by ISSEA for each of the certification categories will be considered as criteria for certification and inclusion in the registry.



ISSEA may directly administer, outsource, or authorize third-party organizations to administer the SSE-CMM Appraiser and/or Professional Examinations in conjunction with or independently of the presentation of the SSE-CMM training. In order to meet the requirements to ensure integrity of the examination, the specific requirements listed in detail below must be met.

Requirements for the Administration of the Examination

Ensuring the integrity of the examination process is an essential part of the ISSEA certification process. In order to ensure integrity, ISSEA examination administrators, outsourced providers, or third party providers must all meet specific minimum requirements. These requirements include:

1. Mechanisms to ensure the confidentiality of the exam;
2. Proof of competency of the examination proctors;
3. Ensuring all persons involved in the examination process will be thoroughly instructed on the mechanisms essential to ensuring the integrity of the examination process; and
4. Mechanisms to ensure the protection of personal information regarding the examination applicants.

Third party organizations desiring to administer the examination must request authorization in writing from ISSEA, detailing the provisions taken to ensure integrity of the examination in accordance with the above requirements.

Examination Proctor Requirements

ISSEA shall ensure that examination proctors of ISSEA examination administrators, outsourced, and third-party providers shall meet the requirements of the certification body based upon applicable standards and other relevant documents.

ISSEA shall ensure that the level of competence of the examination proctor is adequate . As a minimum, examiners shall:

1. Be familiar with the SSE-CMM Appraisal certification scheme;
2. Have a thorough knowledge of the examination methods and examination documents;
3. Be able to communicate effectively both in writing and orally (through an interpreter if necessary) in the language of the examination, and



4. Be free from any personal or special interest so that they can make impartial and non-discriminatory judgments (assessments).

Impartial Examination Validation/Grading Process

ISSEA will take appropriate measures to ensure that objectivity and impartiality of the examination is not compromised. All examination results will be reviewed and validated independently by the ISSEA certification committee.

Certification Process

Application

ISSEA, as the certifying body shall develop and shall provide to applicants a current detailed description of the certification process. The certification process descriptions will:

1. Provide information relevant to each certification scheme (including fees),
2. Provide information regarding the requirements for certification, the applicants' rights, and the duties of a certified person, which includes a code of conduct, as appropriate.

ISSEA requires the completion of an application (Appendix B and C), signed by the applicant seeking certification, which will include:

1. The scope/level of the desired certification;
2. A statement that the person agrees to comply with the requirements for certification and to supply any information needed for the evaluation;
3. Details of relevant qualifications (e.g. education, work experience), confirmed and supported by evidence, and
4. General information on the applicant, e.g. name, address, and other information required to sufficiently identify the person.

ISSEA shall ensure that the personal data and other certificates do not inappropriately influence the certification evaluation.



Evaluation

ISSEA, as the certifying body, shall review each application for certification to ensure:

1. The certification body has the capability to deliver the requested certification in respect of the scope and level of the candidate's qualifications, training, and/or experience.
2. The certification body is aware of and can, within reason, accommodate any special needs of applicants, such as language and/or disabilities;

ISSEA, as the certification body, shall examine candidates' knowledge, skills, and/or ability based on the requirements of the scheme, by written, oral, practical, observational or other evaluation processes. ISSEA has developed and implemented reporting procedures that ensure the performance and results of all the evaluation, including the performance and results of examinations, are documented in an appropriate and comprehensible manner.

All evaluation criteria and results shall be made available to all interested or involved parties.

Required Documentation

At a minimum, applicants for all certifications will provide:

1. Application for certification of the type and at the level requested;
2. Copy of professional credentials;
3. Proof of successful completion of the ISSEA-approved examination at the required level;
4. Copy of educational credentials, including the ISSEA-approved SSE-CMM appraisal methodology training and/or participation in a recognized academic program or completion of a recognized degree program. Documentary evidence may include copy of diploma, copy of training completion certificate, and/or school transcript.

Use of current information is required.

Certification Decisions

ISSEA, as the Certification Body, will render certification decisions.



Re-Certification

It is essential for security professionals to remain up-to-date on the latest technologies, concepts, threats, and countermeasures. Regular re-certification ensures that security professionals maintain their knowledge and skills over time.

Once certification at any level either as an SSE-CMM Appraiser or in the professional certification program, all recipients of certification are required to maintain their skills through ongoing experience and professional/academic development.

Re-certification will be required every three years at a minimum in order to maintain status. A request for an upgrade to a higher level of certification may occur at any time. To re-certify, individuals must provide proof of continuing education and participation in security as a profession.

Certificates

Upon successful completion of the criteria for award of certification under the SSE-CMM Appraiser Certification Program or the Professional Certification Program, ISSEA will provide the certified individual with an official paper certificate reflecting the appropriate level of certification.

Appeals and Complaints

Complaints against the actions or conduct of the ISSEA Certification Board will be submitted in writing to ISSEA care of the President of ISSEA or the Chairman of the Certification Working Group. Each complaint or appeal will be reviewed, investigated, and resolved in a timely manner through a formal documented process.

Appeals against adverse certification may be made on the following decisions:

- Refusal to grant initial certification;
- Refusal to grant the continuation of a certification;
- Refusal to grant the upgrade of a certification;
- Reduction in certification level;
- Cancellation; or
- Suspension.



SSE-CMM Appraiser Certification Requirements

To best accommodate each applicant and distinguish his/her individual credentials, grades of certification have been developed. These are dependent upon the successful completion of the ISSEA-approved and maintained examination affiliated with that level and the level of professional experience attained.

An individual may move up through each category of Certification according to qualifications and suitability, or may enter the Program at an appropriate higher category. Each move to a higher status requires a separate application and a granting of the higher status. Such members then also hold lower designations in their Certification Registry file maintained by ISSEA.

Granting of an Appraiser or Lead Appraiser upon an initial application does not accord the automatic granting of lower categories to the successful applicant.

1. *SSE-CMM Entry-Level Appraiser* –

This certification is considered the entry-level grade for individual appraisers and is designed for individuals seeking to gain appraisal experience by participating in SSE-CMM appraisals. An entry-level appraiser certification may not authorize an individual to lead an appraisal team.

It recognizes that a candidate has satisfied the basic requirements, but has not necessarily performed SSE-CMM appraisals. Attainment of this level authorizes participation on an appraisal team.

An applicant shall satisfy the following requirements:

- a. Education: Applicants shall have, at a minimum, completed a secondary school education (12 years full-time schooling or equivalent) that may lead to admittance into a program of higher education or equivalent. Higher education credentials must be obtained from an institution that has been accredited by a nationally or regionally recognized accreditation body. Proof of relevant security-related education is highly recommended, but not essential.
- b. Training: Successful completion of an SSE-CMM model and appraisal introductory training course is highly recommended and this requirement will be vacated only on a case-by-case basis. In this case, applicants must provide proof of other relevant security and/or CMM related training, as appropriate.
- c. Examination: Successful completion of the ISSEA-accredited examination. (In selected situations, individuals may



demonstrate competency at the entry level by passing the ISSEA accredited examination without a specific requirement to attend ISSEA approved training.)

- d. Professional Experience: As this is the initial level of appraiser certification, the applicant is not required to provide declaration of prior SSE-CMM or similar appraisal experience. The applicant will, however, provide declaration of two or more years of relevant experience in security, disciplines with embedded security activities, and/or the application of capability maturity models. A resume or similar document providing information on professional experience, positions held, and areas of responsibility may be used as objective evidence to satisfy the relevant work experience and support the field of experience selected. Documentation provided must include complete contact information for each position held.

Each person shall sign a personal declaration to indicate that the information contained in the application and attachments is verifiable and accurate to the best of his/her knowledge. In addition, the personal declaration will indicate that the applicant currently complies with, and will continue to comply with, the Code of Conduct for SSE-CMM Appraisers.

Falsification of information shall prevent certification.

2. SSE-CMM Appraiser –

This certification is considered the intermediate grade and is designed for individuals who have gained appraisal experience and have demonstrated the ability to understand and apply the SSE-CMM appraisal methodology, or similar security appraisal methodology, either alone or as a member of a team.

It recognizes that a candidate has satisfied the basic requirements AND has demonstrated the ability to perform all or any part of an SSE-CMM appraisal, alone or as a member of a team, to include leading an appraisal.

An applicant shall satisfy the following requirements:

- a. Education: Applicants shall have, at a minimum, completed a secondary school education (12 years full-time schooling or equivalent) that may lead to admittance into a program of higher education or equivalent. Higher education credentials must be obtained from an institution that has been accredited by a nationally or regionally recognized accreditation body. Proof of relevant security-related academic higher education is highly recommended, but not essential. Relevant experience may be substituted for advanced academic requirements. (See Section d. below.)



- b. Training: Successful completion of an SSE-CMM model and appraisal ISSEA-accredited training course or equivalent training. The applicant must demonstrate that he/she has successfully completed the appropriate level of training by passing the ISSEA-accredited examination for this certification level or by providing alternative certification. Certificates of attendance are not sufficient. Applicants may also provide proof of other relevant security and/or CMM related training, as appropriate.
- c. Examination: Successful completion of the ISSEA-accredited examination or other certification or examination as authorized upon individual review by ISSEA. (In selected situations, individuals may demonstrate competency at the entry level by passing the ISSEA accredited examination without a specific requirement to attend ISSEA approved training.)
- d. Professional Experience: At this level, the applicant is required to provide declaration of a
 - 1. Total of five years SSE experience or equivalent security experience directly or within disciplines with embedded security activities,
 - 2. two years related practical security appraisal experience,
 - 3. and participation/management in a minimum of three appraisals or similar appraisal experience and/or the equivalent application of capability maturity models.

In order to be considered eligible, at least part or all of the experience must have occurred in the three years prior to the application. At least two of the appraisals must have included at least two days of on-site activity.

A resume or similar document providing information on professional experience, positions held, and areas of responsibility may be used as objective evidence to satisfy the relevant work experience and support the field of experience selected. Documentation provided must include complete contact information for each position held.

Each person shall sign a personal declaration to indicate that the information contained in the application and attachments is verifiable and accurate to the best of his/her knowledge. In addition, the personal declaration will indicate that the applicant currently complies with, and will continue to comply with, the Code of Conduct for SSE-CMM Appraisers.

Falsification of information shall prevent certification.



3. *SSE-CMM Lead Appraiser –*

This level of certification is considered the advanced grade and is designed for individuals with SSE-CMM appraisal, or similar security appraisal, experience who have demonstrated the ability to perform all or part of an appraisal alone or as a member of a team. Specifically, lead appraisers are eligible to lead appraisals of greater complexity. A lead appraiser is required for all appraisals leading to an approved organizational level of SSE-CMM maturity.

It recognizes that a candidate has satisfied the basic requirements, has demonstrated the ability to perform all or any part of an SSE-CMM appraisal alone or as a member of a team AND has demonstrated the ability to manage an appraisal team and coordinate all aspects of a complete SSE-CMM appraisal.

An applicant shall satisfy the following requirements:

- a. Education: Applicants shall have, at a minimum, completed a secondary school education (12 years full-time schooling or equivalent) that may lead to admittance into a program of higher education or equivalent. Higher education credentials must be obtained from an institution that has been accredited by a nationally or regionally recognized accreditation body. Proof of relevant security-related education is highly recommended, but not essential. Relevant experience may be substituted for advanced academic requirements. (See Section d. below.)
- b. Training: Successful completion of an SSE-CMM model and appraisal training course or other equivalent training. The applicant must demonstrate that he/she has successfully completed the appropriate level of training by passing the ISSEA-accredited examination or by providing alternative certification. Certificates of attendance are not sufficient. Applicants may also provide proof of other relevant security and/or CMM related training, as appropriate.
- c. Examination: Successful completion of the ISSEA-accredited examination or other certification determined by ISSEA to be sufficient. (In selected situations, individuals may demonstrate competency at the entry level by passing the ISSEA accredited examination without a specific requirement to attend ISSEA approved training.)
- d. Professional Experience: At this level, the applicant is required to provide declaration of a:
 1. total 10 yrs SSE or equivalent security experience or experience in disciplines with embedded security



activities and/or advanced training or academic degree,

2. five years practical security appraisal experience
3. and/or minimum of seven appraisals and/or the equivalent application of capability maturity models.

In order to be considered eligible, at least part or all of the experience must have occurred in the three years prior to the application. At least five of the appraisals must total 25 days and three of the five must include at least two days of on-site appraisal activity.

A resume or similar document providing information on professional experience, positions held, and areas of responsibility may be used as objective evidence to satisfy the relevant work experience and support the field of experience selected. Documentation provided must include complete contact information for each position held.

Each person shall sign a personal declaration to indicate that the information contained in the application and attachments is verifiable and accurate to the best of his/her knowledge. In addition, the personal declaration will indicate that the applicant currently complies with, and will continue to comply with, the Code of Conduct for SSE-CMM Appraisers.

Falsification of information shall prevent certification.

Recertification

The requirements for re-certification are the same as for the original application for Certification and must be supported by a new application and proof of eligibility for the Certification Program. Where ISSEA Certification Program Registry files contain records of previous applications and approved Certification, the applicant need only update that information.

Grandfathering Requirements for the SSE-CMM Appraiser or SSE-CMM Lead Appraiser

A Grandfathering period of one year from the date of program implementation will be established. All applications for grandfather status will be reviewed by a review committee established by the ISSEA Certification Working Group and approved by the ISSEA Board of Directors:

An individual will be awarded recognition as an **SSE-CMM Appraiser** if they meet the following criteria:



1. Experience and Education: Acceptable proof of experience includes no less than five years experience in the SSE-CMM Appraisal Methodology and/or other recognized security appraisal methodology; participation in the development or ongoing maintenance of the SSE-CMM model and associated processes; contributions to the field of security (e.g., publications, presentations); exposure to other capability maturity models and their application in an appraisal process. Acceptable proof of education includes successful completion of a bachelor's program in a relevant field of study (e.g., Information Systems, Information Systems Security, Information Technology Management) and/or successful completion of independent commercial certifications (CISSP, GIAC, ISSEP, and others).
2. Professional Reference: The applicant must provide a letter of reference from his/her employer attesting to the qualifications for certification. Additionally, a letter from another grandfathered or certified SSE-CMM Appraiser or SSE-CMM Lead Appraiser may be submitted.
3. Ethics Statement: The applicant must sign the ISSEA Code of Ethics statement found on the back of the application.
4. Application: The applicant must complete and submit an application and meet the eligibility requirements in place at the time of the application.

An individual will be awarded recognition as an **SSE-CMM Lead Appraiser** if they meet the following criteria:

1. Experience and Education: Acceptable proof of experience includes no less than ten years experience in the SSE-CMM Appraisal Methodology and/or other recognized security appraisal methodology; participation in the development or ongoing maintenance of the SSE-CMM model; valuable contributions to the field of security (e.g., publications, presentations, security tools development); application of other capability maturity models in an appraisal process. Acceptable proof of education includes successful completion of a post-graduate program in a relevant field of study and/or successful completion of independent commercial certifications (CISSP, GIAC, and others).
2. Professional Reference: The applicant must provide a letter of reference from his/her employer attesting to the qualifications for certification. Additionally, a letter from another grandfathered or certified SSE-CMM Appraiser or SSE-CMM Lead Appraiser may be submitted.
3. Ethics Statement: The applicant must sign the ISSEA Code of Ethics statement found on the back of the application.
4. Application: The applicant must complete and submit an application and meet the eligibility requirements in place at the time of the application.



Exceptions

ISSEA has the responsibility for establishing a mechanism for handling exceptions to the above processes of certification and grandfathering.

Control of Non-Conforming Activities

ISSEA has procedures to be implemented should it establish that any aspect of the training and/or certification activities does not conform with its own procedures or the agreed upon requirements.

The procedure ensures that:

- a. Responsibilities and authorities for the management of nonconforming activities are designated;
- b. The actions to be taken when a nonconformance is identified are defined;
- c. An evaluation of the significance of the nonconforming activity is made;
- d. Activity is halted if necessary;
- e. Remedial actions are taken promptly;
- f. Where appropriate, the nonconforming results or certifications already issued are recalled;
- g. The responsibility for resumption of activity is defined;
- h. Complete records of all nonconforming activities and remedial actions are maintained.

Fee Structure

Fee schedules are set by ISSEA. Please refer to the ISSEA Web Site for the contact numbers to obtain additional information.

ISSEA Membership

A certification candidate is not required to be a member of ISSEA in order to obtain certification; however, ISSEA encourages the consideration of advantages in terms of access to other professionals, conference participation, and sponsorship.

Additional information on ISSEA membership is provided on the ISSEA website.



References

1. ISO/IEC 17024, Draft International Standard, General Requirements For Bodies Operating Certification Schemes For Persons
2. ISO 9001, Quality Management Systems – Guidelines for Performance Improvements
3. ISO 21827, Systems Security Engineering – Capability Maturity Model
4. Systems Security Engineering – Capability Maturity Model Appraisal Methodology, V. 2.0.

Definitions

PROVIDER: A body (organization or firm, public or private) that undertakes the design and conduct of a training and/or certification scheme.

EQUIVALENT SECURITY APPRAISAL EXPERIENCE: Experience in other process-oriented security appraisal methodologies, such as the IA-CMM.



Appendix A: Code of Ethics

As a certified SSE-CMM Appraiser or an SSE Professional, I pledge to uphold professional principles in the fulfillment of my responsibilities.

In promoting a high standard of ethical conduct, I shall:

1. Act professionally, accurately, and in an unbiased manner.
2. Endeavor to raise the competence and prestige of the security profession.
3. Assist those with whom I work, in my employ, or under my supervision in developing their skills specific to their chosen profession.
4. Not represent conflicting or competing interests and understand my responsibility to disclose to any client or employer any relationships that may influence my judgment.
5. Not discuss or disclose any client information unless authorized in writing by the client.
6. Not accept any inducement, commission, gift or other benefit from client organizations, their employees, or any interested part or knowingly allow colleagues to do so.
7. Not intentionally communicate false or misleading information that may compromise the integrity of any appraisal or the certification process.
8. Not act in any manner that would prejudice the reputation of the certification body or the certification process, and shall cooperate fully with any inquiry into any alleged breach of this code.
9. Conduct myself professionally, with honesty, accuracy, fairness, and responsibility to my clients and my colleagues.
10. Preface any public statements with a clear disclaimer on whose behalf they are made.
11. Take care that credit for successful work of other is given to those to whom it is due.
12. Not misrepresent my own or any other individual's qualifications, competence, or experience, nor undertake appraisal or other system security engineering related work beyond my qualifications.
13. Not accept compensation from more than one party for the same services without the consent of all parties concerned.



-
14. Not accept retainers, commissions, or valuable considerations from any unauthorized parties in exchange for offering confidential or sensitive information or disclosures that related in any way to clients, employers, or the certification process.
 15. Not serve any private or special interest in the performance of my services as an appraiser.



Appendix B: SSE-CMM Appraiser Examination Registration Form and Application for Certification

The first step in the registration and application process is to submit a formal request containing the following information:

1. Name, Address, Phone Number, eMail
2. Title/Position
3. Employer, Business Address, Phone Number, eMail
4. Background Information:
 - i. Ever convicted of a felony, a crime based on dishonesty (felony or misdemeanor involving lying) or a Court Martial in military service, or is there a pending felony charge?
 - ii. Ever had a professional license, certification, membership or registration revoked, or been censured or disciplined by any professional organization or government agency?
 - iii. Ever been involved, or publicly identified, with hackers or hacking?
 - iv. Ever been known by an alias or pseudonym?
5. A physical or other disability that might require special arrangements.

The applicant must meet the following requirements to sit for the examination:

1. Subscribe to the ISSEA Code of Ethics and validate this with a signed statement.
2. Meet the education, training and/or experience requirements. Applicant must provide dates and locations of education, training, and experience meeting the minimum requirements.

By registering for the examination and certification, the applicant will affirm understanding of the following policies:

1. Cancellations and Refunds: If the exam size of any location is exceeded, registrations will be accepted based on the earliest postmark date when payment in full of registration fees is received. The sponsoring agency has the right to cancel any examination 5 days in advance if attendance is not sufficient.
2. Examination Retakes: It is the policy of ISSEA to prohibit the retaking of any SSE-CMM certification exam by an application earlier than 90



days following the failed examination. A certification holder may not retake the examination if de-certified by ISSEA and prohibited from being recertified.

3. Confidentiality and Copyrights: ISSEA requires applicants to verify adherence to the Code of Ethics. All information related to the examination will be treated as confidential, whether provided directly by ISSEA or by another source.

In order to be issued a certificate, the applicant must:

1. Pass the examination;
2. Submit a signed endorsement*.

*Endorsement: another qualified professional with knowledge of information systems or an officer of the candidate's corporation can be used to validate the candidate's professional experience. The endorser will attest that the candidate's assertions regarding professional experience are true to the best of their knowledge, and that the candidate is in good standing within the information security industry.

Upon receipt of the Endorsement Form and barring a random audit of the candidate's professional experience, the SSE-CMM credential should be awarded within five business days, with a formal notification sent via e-mail.



Appendix C: Application for Review and Approval of Third-Party SSE-CMM Training and/or Authority to Administer the SSE-CMM Appraiser Exam

The first step in the application procedure for review and approval of third-party SSE-CMM training and/or authority to administer the SSE-CMM Appraiser Exam is submission of a letter of application by the requesting body. The purpose is to enable ISSEA to judge the eligibility of the training program and/or the request for authority to administer the SSE-CMM Appraiser Exam for review and approval. The letter of application should contain the following minimum information:

1. Confirmation of the third party status of the program.

A third party is independent of the parties involved in certification, i.e., the supplier ("first party") interests and the purchaser ("second party") interests. Describe how the sponsoring body qualifies as a third party, and describe the interests represented on the body's governing board.

2. Description of the training and a copy of the publicly available documents describing the training program; i.e., training materials, syllabus.

3. Copies of descriptive brochures, application forms, advertisements, etc.

4. A brief description of the training program, including a list of the standard(s) utilized.

5. A description of the methods used to ensure integrity of the examination process; i.e., protection of the examination material, proctoring, protection of completed exams, and protected transmission of test results.

The letter of application should be submitted to the Program Management Office, International Systems Security Engineering Association.