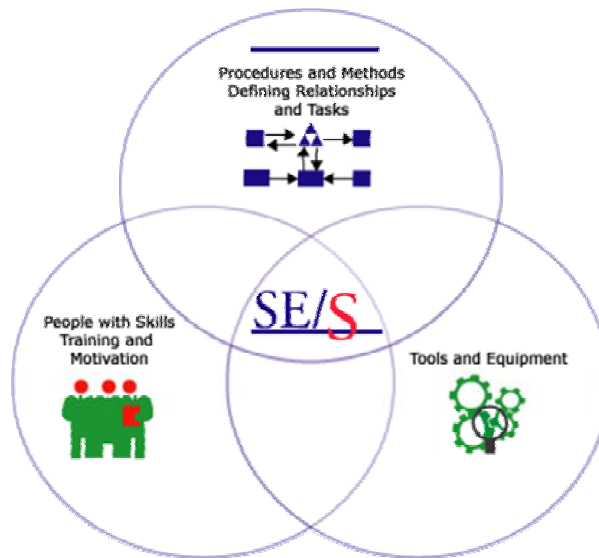


Software Engineering Security Management Curriculum

Course Outlines

Version 2.5
February 2004



Transition Partner for CMMI[®] SCAMPISM Appraisal Service
Carnegie Mellon University Software Engineering Institute

TABLE OF CONTENTS

1. QUALITY ASSURANCE INSTITUTE..... 1

1.1 QUALITY ASSURANCE INSTITUTE MIDDLE EAST AND AFRICA (QAI MEA) 1

1.2 OUR APPROACH 1

1.3 QAI MEA SERVICES 1

1.4 INDIVIDUAL CERTIFICATIONS 2

1.5 CORPORATE APPRAISALS 3

1.6 KNOWLEDGE TRANSFER PARTNERS: 3

2. INFORMATION SECURITY MANAGEMENT 1

2.1 PREREQUISITE KNOWLEDGE 1

2.2 COURSE OBJECTIVES 1

2.3 COURSE DESCRIPTION 1

2.4 COURSE TOPICS 1

3. INFORMATION SECURITY AWARENESS PROGRAM..... 2

3.1 PREREQUISITE KNOWLEDGE..... 2

3.2 COURSE OBJECTIVES 2

3.3 COURSE DESCRIPTION 2

3.4 COURSE ORGANIZATION 2

3.5 COURSE TOPICS 2

4. INFORMATION SECURITY RISK MANAGEMENT 3

4.1 PREREQUISITE KNOWLEDGE..... 3

4.2 COURSE OBJECTIVES 3

4.3 COURSE DESCRIPTION 3

4.4 COURSE ORGANIZATION 3

4.5 COURSE TOPICS 3

5. INTRODUCTION TO INFORMATION SECURITY..... 5

5.1 PREREQUISITE KNOWLEDGE..... 5

5.2 COURSE OBJECTIVES 5

5.3 COURSE DESCRIPTION 5

5.4 COURSE ORGANIZATION 5

5.5 COURSE TOPICS 5

6. SECURITY ENGINEERING PROCESS MANAGEMENT..... 7

6.1 PREREQUISITE KNOWLEDGE..... 7

6.2 COURSE OBJECTIVES 7

6.3 COURSE DESCRIPTION 7

6.4 COURSE ORGANIZATION 7

6.5 COURSE TOPICS 7

7. WRITING INFORMATION SECURITY POLICIES AND PROCEDURES..... 9

7.1 PREREQUISITE KNOWLEDGE..... 9

7.2 COURSE OBJECTIVES 9

7.3 COURSE DESCRIPTION 9

7.4 COURSE ORGANIZATION 9

7.5 COURSE TOPICS 9

1. Quality Assurance Institute

The Quality Assurance Institute was founded in 1980 in the United States of America. QAI's founding objective was and remains to provide leadership in improving quality, productivity, and effective solutions for process management in the information services profession. It is a worldwide membership organization serving over 1000 corporate members, organized to share state-of-the-art methods, tools, and techniques. The combined experience of QAI experts and of our member companies provides an impressive body of knowledge, a reservoir for our members to share. QAI has transformed this knowledge and experience into a "how-to" approach that is being taught worldwide.

1.1 Quality Assurance Institute Middle East and Africa (QAI MEA)

The QAI MEA was established in January 2001 to serve primarily the Middle East and African countries. It is an independent organization with a full partnership and access to all resources and services of the QAI global organization. Although the mission, objectives and approach are shared with the global organization, the QAI MEA has tailored and adapted its services to the local environment and culture to better serve our customers.

We take pride in being one of the first professional organizations to recognize the need for quality assurance and to have the vision to be exclusively devoted to the information technology profession. QAI provides leadership and state-of-the-art solutions in the form of consulting, education and training services, and assessments.

1.2 Our Approach

QAI takes a business-oriented approach to Managing Quality. It recognizes the close working relationship that must exist between information technology services and their internal and external customers. The approach shows methods for improving the processes within information technology organizations, leading to improved products and services.

Our approach takes into account the need of many organizations to re-establish credibility with their customers due to the past performance. It guides these organizations in building an environment where high quality products are completed on time and within budget. Our assessment and certification programs can also attest and provide evidence that their organization is operating effectively and efficiently.

1.3 QAI MEA Services

QAI MEA focuses on three major service channels, corresponding to the key quality components of any IT installation:

- Quality assurance
- Project management
- IT Service Management
- IT Security

Within each service channel, QAI MEA provides distinct levels of service:

- Appraisals, assessments and reviews against the major standards and models,
- Education and training through formal courses, e-Learning courses, workshops and seminars,
- On-site Consulting to assist clients in reaching their goals and objectives expediently and economically.

QAI MEA engages only highly qualified and skilled staff in order to ensure the highest quality service expected by our customers. We have on our staff certified assessors, project managers, and trainers with proven records of accomplishment with our extensive client base. We are proud to participate and lead in the community functions of the region. We are active participants in Dubai Quality Group and Dubai Quality Award activities.

1.4 Individual Certifications

1.4.1 Certified Software Quality Analyst (CSQA)

Acquiring the designation of Certified Software Quality Analyst (CSQA) indicates a professional level of competence in the principles and practices of quality assurance in the IT profession. CSQA certification is a highly respected attestation of skills in this critical area of information technology.

1.4.2 Certified Software Test Engineer (CSTE)

The Certified Software Test Engineer (CSTE) Program is intended to establish standards for initial qualification and provide direction for the testing function through an aggressive educational program.

1.4.3 Certified Software Project Manager (CSPM)

The Certified Software Project Manager program is intended to establish standards for initial qualification, and continuing improvement of professional competence. This certification program helps to:

- Define the tasks (skill domains) associated with software project management activities in order to evaluate mastery of these activities.
- Demonstrate an individual's willingness to improve professionally.
- Acknowledge attainment of an acceptable standard of professional competency.
- Aid organizations in selecting and promoting qualified individuals.
- Motivate personnel having software project management responsibilities to maintain their professional competency.
- 6. Assist individuals in improving and enhancing their organization's software project management programs (i.e., provide a mechanism to lead a professional).

1.4.4 Examination

Candidates for certification must pass a four-part written examination in order to obtain certification. The examination tests the candidate's knowledge and practice of the skill areas defined in the respective [CSQA Body of Knowledge](#) or [CSTE Body of Knowledge](#). There are three certification centers in the Middle East:

[Etisalat Academy](#), Dubai, United Arab Emirates

[Takniat Training and Technology Transfer](#), Riyadh, Saudi Arabia

[International Information & Communication Technology Center](#), Cairo, Egypt

Please refer to <http://www.softwarecertifications.com> for more information

1.5 Corporate Appraisals

QAI MEA is a Transition Partner for the Capability Maturity Model[®] Integration (CMMI[®]) for the Standard CMMI[®] Appraisal Method for Process Improvement (SCAMPISM). The SCAMPI method is a diagnostic tool that supports, enables, and encourages an organization's commitment to process improvement. The method helps an organization gain insight into process capability or organizational maturity by identifying process strengths and weaknesses relative to one or more of the [CMMI[®] models](#).

1.6 Knowledge Transfer Partners:

[Carnegie Mellon University Software Engineering Institute](#) USA

[Etisalat Academy](#), Dubai, United Arab Emirates

[Takniat Training and Technology Transfer](#), Riyadh, Saudi Arabia

[International Information & Communication Technology Center](#), Cairo, Egypt

[Quality Assurance Institute](#), USA

[Quality Assurance Institute](#), India

2. Information Security Management

2.1 Prerequisite knowledge

- Participants in this course should have a degree in computer science/engineering or equivalent work experience.
- Participants will have successfully completed predecessor Foundation Course.

2.2 Course objectives

You will learn:

- IT security concepts and terminology
- How to apply process concepts across the spectrum of IT related activities and artifacts
- Obtain common understanding and agreement to security processes that support specific business objectives
- Identify best practices for managing quality and security
- Implement a security software process improvement initiative in your organization

2.3 Course Description

The drive toward pervasive interconnectivity and interoperability of networks, computers, applications, and even enterprises is creating a more pivotal role for security in all systems and products. The focus of security has moved from safeguarding classified government data, to a wider application, including financial transactions, contractual agreements, personal information, and the Internet. As a result, it is necessary that potential security needs are considered and determined for any application. Examples of needs to consider include confidentiality, integrity, availability, accountability, privacy, and assurance.

Course organization

- The course consists of ten modules, each four hours in duration
- Modules will be taught over a five day period, two modules per day

2.4 Course Topics

1. General Security Considerations
2. Introduction to the System Security Engineering Capability Maturity Model (SSE-CMM)
3. Using the SSE-CMM
4. The System Security Appraisal Method (SSAM)
5. Comparison of Standards
6. ISO 17799
7. How to Write Information Security Policies and Procedures

3. Information Security Awareness Program

3.1 Prerequisite Knowledge

Participants in this course should have a basic knowledge of information security principles. There are no other prerequisites.

3.2 Course Objectives

You will learn:

- Information Security Awareness concepts and terminology
- How to plan and organize an Information Security Awareness program in your organization
- How to focus and tailor your program to your organization's specific needs
- Identify best practices for developing, implementing and maintaining your awareness program
- Develop metrics to measure the effectiveness of your awareness program

3.3 Course Description

This course addresses one of the most important and often ignored aspects of information security. Participants will learn the importance of developing an information security awareness program in their organizations and how to go about developing and implementing one. Participants will walk through the steps of identifying areas inside their organizations that require an awareness program. Participants will learn how to develop an information security awareness program according to their organization's needs and capabilities. Participants will understand the various methods of communicating the security awareness message to every part of the organization.

3.4 Course organization

The course consists of four modules of four hours each that are taught over a two day period.

3.5 Course Topics

1. Considerations Before Developing the Information Security Awareness Program
2. Implementing the Information Security Awareness Program
3. What to put into your presentation
4. Additional Considerations
5. ISAP Evaluation
6. Human Firewall Project
7. The Top Ten Most Common Mistakes
8. Summary and Conclusions

4. Information Security Risk Management

4.1 Prerequisite Knowledge

Participants in this course should have a basic knowledge of information security management principles. There are no other prerequisites.

4.2 Course Objectives

You will learn:

- Information security risk management concepts and terminology
- How to plan and organize an information security risk management program in your organization
- How to determine your organization's risk posture
- How to identify your organization's risks and build mitigation plans to address those risks
- How to implement a phased approach to addressing your organization's information security risk

4.3 Course Description

This course addresses one of the key aspects of information security: risk management. Many organizations focus solely on infrastructure weaknesses and fail to establish the effect on their most important information assets. This leads to a gap between an organization's operational and information technology requirements, placing the assets at risk. Current approaches to information security risk management tend to be incomplete. The first step in managing information security risk is to understand what your risks are. Once an organization has identified its risks, it can build mitigation plans to address those risks. The Information Security Risk Management course endeavors to give students the tools they need to implement an effective information security risk management program in their organizations. Students will learn to build asset-based threat profiles, identify infrastructure vulnerabilities and develop security strategies and plans. At the end of this course students will have the tools necessary to conduct a risk assessment of their organization and implement mitigation strategies.

4.4 Course organization

The course consists of four modules of four hours each that are taught over a two day period.

4.5 Course Topics

1. Managing Information Security Risks
2. Principles and Attributes of Information Security Risk Evaluations
 - 2.1. Select
3. Identifying Organizational Knowledge
4. Creating Threat Profiles
5. Identifying Key Components
6. Evaluation Selected Components
7. Conducting the Risk Analysis

8. Developing a Protection Strategy
9. Practical Applications
10. Information Security Risk Management

5. Introduction to Information Security

5.1 Prerequisite Knowledge

Participants in this course should have a basic knowledge of information technology principles. There are no other prerequisites.

5.2 Course Objectives

You will learn:

- Information Security concepts and terminology
- Understanding of risk management
- Understanding of threats
- How to develop and implement countermeasures
- What role do information security policies, procedures, standards, and guidelines play in an information security strategy
- Understand the ten domain model of information security
- The principles of Internet security
- Gain an understanding of current trends in information security

5.3 Course Description

This is an introductory course for those that are new to the field of information security or whose duties require them to have a basic knowledge of information security principles. This course is useful to managers with information security responsibilities. Participants will be introduced to the terminology of the trade. This course will build the key foundations that will be required as participants continue their information security education. Students will study the basics of risk management and threats to the organization. The course will address the ten domains of information security: Access Control Systems and Methodology, Applications and Systems Development Security, Business Continuity Planning and Disaster Recover Planning, Cryptography, Law, Investigations, and Ethics, Operations Security, Physical Security, Security Architecture and Models, Security Management Practices, and Telecommunications and Network Security. The course will cover the role of policies, procedures, standards, and guidelines. Students will learn about Internet security and how it applies to their daily duties.

5.4 Course organization

The course consists of four modules of four hours each that are taught over a two day period.

5.5 Course Topics

1. Overview of Information Protection Fundamentals
2. The Fundamentals of Risk Analysis
3. Information Security Policies and Procedures
4. Information Security Awareness Programs
5. Standards
6. Common Information System Security Vulnerabilities

7. Introduction to Security Engineering
8. Incident Handling and Forensics
9. Password Management
10. Cryptography
11. Firewalls and Perimeter Defense
12. Information Security: The 10 Domain Approach
13. Maintaining an Information Security Program
14. Information Security Education
 - 14.1. Certified Information Systems Security Professional (CISSP)
 - 14.2. Global Information Assurance Certification (GIAC)
 - 14.3. Certified Information System Auditor (CISA)
 - 14.4. Other educational opportunities

6. Security Engineering Process Management

6.1 Prerequisite Knowledge

Participants in this course should have a basic knowledge of information security principles. There are no other prerequisites.

6.2 Course Objectives

You will learn:

- The System Security Engineering Capability Maturity Model (SSE-CMM)
- How to apply the SSE-CMM to your organization's security engineering activities and measure and define improvement
- How to use the model to evaluate a security provider's security engineering capability
- How to integrate the model into your RFPs
- The benefits of using the SSE-CMM
- Develop metrics to measure the effectiveness of your organization's security engineering activities
- Gain an understanding of the Security Engineering discipline.
- Understand how security is an integral part of the engineering process
- The 11 Process Areas of the model and 60 Security Base Practices.
- How to use the SSE-CMM as a Step-by-Step Guide for Process Improvement and Capability Evaluation
- The System Security Appraisal Method (SSAM) and how to apply it

6.3 Course Description

This course will serve as an introduction to the SSE-CMM. The model was created to provide organizations with a description of what characteristics must exist in their security engineering process in order to ensure good security engineering. The first two days of the course will be devoted to learning the 11 process areas of the model and the 60 security base practices. The third day of the course will focus on how to apply the model to an organization or engineering process and the System Security Appraisal Method (SSAM).

6.4 Course organization

The course consists of four modules of four hours each that are taught over a two day period.

6.5 Course Topics

1. Introduction to the SSE-CMM
2. Key Concepts
3. Model Architecture
4. Using the SSE-CMM
5. Generic Practices
6. Security Base Practices

7. The System Security Appraisal Method (SSAM)
8. Practical applications of the SSE-CMM

7. Writing Information Security Policies and Procedures

7.1 Prerequisite Knowledge

Participants in this course should have a basic knowledge of information security management principles. Participants should have a good command of English language and grammar. There are no other prerequisites.

7.2 Course Objectives

You will learn:

- Information Security management concepts and terminology
- How to plan and organize an Information Security documentation program in your organization
- How to determine your organization's policy needs
- How to develop and implement effective information security policies and procedures according to your organization's specific needs
- Understand the role that policies, procedures, standards and guidelines play in an organization's information security strategy
- How to manage the information security policy and procedure process as a project
- How to develop and implement a documentation review process

7.3 Course Description

This course addresses one of the key aspects of information security: policy. The purpose of information protection is to protect an organization's resources. The cornerstone of any information security strategy is a robust set of policies, procedures, standards and guidelines. Participants will learn the importance of developing an information security documentation program in their organizations and how to go about developing and implementing effective policies and procedures. Participants will understand that providing information protection requires a comprehensive approach that considers areas within and outside the area of information technology. Effective information security often involves sustained process improvement. Participants will focus on the following areas: Information Protection Fundamentals, Writing Mechanics and the Message, Policy Development, Mission Statement, Standards, Writing Procedures, Information Classification, and How to Manage the Process as a Project. Examples of various policies and procedures will be provided.

7.4 Course organization

The course consists of four modules of four hours each that are taught over a two day period.

7.5 Course Topics

1. Overview of Information Protection Fundamentals
2. Writing Mechanics and the Message
3. Policy Development
4. Mission Statement
5. Standards

6. Writing Procedures
7. Information Classification
8. Security Awareness Program
9. Why Manage This Process as a Project?
10. Information Technology: Code of Practice for Information Security Management
11. Determining Your Policy Needs
12. Writing the Security Policies
13. Maintaining the Policies