

Special Interest Group in Security and Information Integrity (SIG²)

Centre for Competency

Information System Security Course Evaluation Methodology

< DRAFT version 0.1 >

Draft for Comment

Special Interest Group in Security and Information Integrity (SIG²) Centre for Competency (CC)

Information System Security Course Evaluation Methodology

This draft is being circulated by SIG² for a 3-month period of public comment (15th April to 30th Jun 2004). It is issued to allow comments by all interested parties in both the SIG² associates (sponsors and members) and the local security communities. All comments will be given consideration after the public comment period prior to the publication of the new edition of the framework.

No copying is allowed, in any form, without prior written permission from SIG² except as permitted under the Copyright Act 1988 or for circulation within organizations participating in the public comment period for briefing purposes.

Electronic circulation is limited to dissemination by e-mail within such organizations.

Draft for Public Comment



© Copyright 2004

< <http://www.security.org.sg> >

Latest date for receipt of comments: 30 Jun 2004

Special Interest Group for Security and Information Integrity (SIG²) Centre for Competency (CC)

Information System Security Course Evaluation Methodology

Prepared by	Reviewed By	Approved By
Khoh Chih Jeun, SIG ² Committee Member, 20 March 2004 Vincent Leong, SIG ² Committee Member, 20 March 2004	Name Designation Date	Aloysius Cheang President, SIG ² 12 April 04

**WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A STANDARD.
THIS DRAFT IS NOT CURRENT BEYOND ITS EXPIRY DATE FOR COMMENTS.**

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication.

No copying is allowed, in any form, without prior written permission from SIG² except as permitted under the Copyright Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

TABLES OF CONTENT

1. INTRODUCTION	6
1.1 Background.....	6
1.2 Document Objective	6
1.3 Document Updates	6
2. EVALUATION METHODOLOGY	7
2.1 Determining Relevancy.....	7
2.2 Courses Rating	8
ANNEX A – Course Evaluation Form.....	10

1. INTRODUCTION

1.1 Background

Organizations today have a barrage of security technologies at their disposal. However, no controls would be effective if the security implementation process is not supported by competent and proficient personnel. Building and maintaining IS (Information Systems) security competency have always been a management challenge and despite the importance of training, there is often very few suitable tools to aid the management in the selection of appropriate trainings and measuring cost effectiveness of these trainings.

In this paper, we proposed an approach to determining training relevancy and provide a common baseline for comparing course effectiveness.

1.2 Document Objective

- To quantify course relevancy to various IS security roles; and
- To provide a ranking system to measure course effectiveness.

1.3 Document Updates

This methodology is reviewed annually by the SIG2 Common Criteria Working Group.

2. EVALUATION METHODOLOGY

This section describes the 2-step evaluation process for all courses sent to SIG2 for assessments.

Each of the courses evaluated shall be classified as described in Section 2.1 to determine its relevancy to the various IS security roles.

Following which, the course is rated according to a common criteria listed in Section 2.2.

An overall rating will be awarded to facilitate comparisons between courses. This overall rating is derived from the median of the ratings awarded to each of the criterion.

All evaluations shall be accompanied by a qualitative assessment detailing course-specific observations and other non-quantifiable information.

2.1 Determining Relevancy

All IS security courses and training are grouped into the following categories:

General Awareness, program which imparts high-level concepts of IS security and general knowledge on using IS resources securely.

Security Planning and Management Concepts, program which focuses in details on IS security principles and strategies. Belonging to this genre are courses on risk assessment methodology, security program designs, secure network infrastructure design and deployment etc.

Domain Specific Knowledge, program which imparts low level know-how necessary for the implementation of various security controls. Courses of this genre include platform/ technology-specific training such as firewall security administration.

Similarly, major IS security roles can be grouped into the following categories:

Senior Management, sets IS security directions and makes decisions on IS security budget.

IS Security Program Manager, ensures the implementation of risk management for business IS systems and is directly responsible for these systems' security.

IS Security Consultant, supports the IS security program manager in the roll-out of IS security projects and works directly with the IS Administrator and Operators in ensuring compliance to organization's IS policies.

IS Administrator and Operator, (e.g., network, system, application, and database administrator; computer specialist; data security analyst), manages and administers security controls for IS systems.

End user, uses the IS systems.

Relevancy is determined by the following matrix:

	General Awareness	Planning & Management Concepts	Domain Specific
Senior Management	Highly Relevant	Relevant	-
IS Security Program Manager	Relevant	Highly Relevant	Relevant
IS Security Consultant	Relevant	Highly Relevant	Highly Relevant
IS Administrator and Operator	Relevant	Relevant	Highly Relevant
End User	Highly Relevant	-	-

For example, an AIX Security Administration course is classified as a domain specific course and is highly recommended for IS Security Consultant and IS Security Administrator and Operator. On the other hand, a security awareness course on Home Computing would probably see better ROI from End User than from an IS Security Consultant.

2.2 Courses Rating

The courses are evaluated according to the following criteria:

Course Content

- The course should have a clear objective and is relevant to the IS security industry.

- There must be agreement between the course objectives and the course content
- The course should equip the student with adequate knowledge to tackle real world issues.

Course Conduct

- The course should be presented in an organised manner.
- The instructor should communicate knowledge of the subject matter and make difficult concepts understandable.
- The instructor should simulate interest in the subject area
- The instructor should demonstrate a positive attitude towards participation

Cost Effectiveness

- Quality of the course content
- Quality of the course material
- Quality of the instructor
- Quality of the course facilities

For the above selection criteria, a rating of 1 to 5 is given with 5 as the best award for each category. The form in Annex A shall be used for all course evaluation.

ANNEX A – Course Evaluation Form

Course Evaluation Form					
Course Title:					
Organizer:					
Instructor:					
Time/Date:					
Prerequisite:					
Course Categories: <i>(General Awareness/Planning & Management/ Domain Spec.)</i>					
Relevancy: <i>(Highly Relevant - Senior Management, Relevant - IS Security Consultant etc.)</i>					
Course Content	Excellent (5)	Good (4)	Average (3)	Fair (2)	Inadequate (1)
Clarity of course objectives					
Agreement between course objectives and course content					
Relevancy of course content to real world issues					
Detail Coverage of Subject Topic					
Course Content Rating					
Course Conduct	Excellent (5)	Good (4)	Average (3)	Fair (2)	Inadequate (1)
Organisation and the manner of the conduct of the course					
Knowledge communication of the subject matter					
Making difficult concepts understandable					

Simulating interest in the subject area					
Demonstrating a positive attitude towards participation					
Course Conduct Rating					
Cost Effectiveness	Excellent (5)	Good (4)	Average (3)	Fair (2)	Inadequate (1)
Course Duration					
Quality of the course content					
Quality of the course material					
Quality or Subject Knowledge of the instructor					
Quality of the course facilities					
Cost Effectiveness Rating					
Overall Rating					