PROJECT REPORT

APEC and DCITA

Final Status Report

TEL 01/2007 Information Security Certifications Assessment Guide

APEC Publication Number:
APEC#207-TC-01.2

Presented by SIFT to DCITA
Date: 23rd May, 2007

contents

figures

Originated in Australia.

PROJECT OBJECTIVES

The project has developed an Information Security Skills Certification Guide that can be delivered to both the public and private sectors. In particular it helps three different sectors

- It is designed to help SMEs develop an understanding of the issues surrounding security certifications in order to help them choose security employees or suppliers.
- It will help individuals to understand the most appropriate certifications they should seek in order to achieve the best results for their career.
- It will help educational institutions help and guide their students towards security certifications and also help then understand how certifications align with their current curriculum.

The objectives of the Guide are as follows:

- To provide detail on certification content in order to assist information security professionals in selecting the appropriate certification for their job role and career.
- To provide an accepted point of reference with which to compare and contrast certification schemes currently available.
- To increase the confidence level of consumers/employers in knowing when help is required for information security, and where to find the right professionals to do the job.
- To serve the role of informing consumers/employers and professionals to allow them to decide on the most appropriate program for their needs.
- To include further references to sources of knowledge that may not be covered/referenced by current certifications, such as new and accepted references to best practice.
- NOT to promote specific certification schemes.

The Guide has been developed and deployed as an Internet portal, and is to be used as the medium for disseminating the required information to professionals and consumer/employers. As an Internet portal it will provide broad access to the widest audience possible.

The information contained in the web site is advice and guidance for a range of users. Through this web site, APEC will be providing a service to everyone in the region by making this resource available and cementing its position as a helpful and relevant organisation. It will also be helping to attain the goals it has set itself on both information & IT security and human resource development.

PROJECT METHODOLOGY

This project was developed using normal project management processes. The stages in the project were as follows:

- Project Initiation
- Develop Project Methodology
- Research Certifications
- Develop Certification database
- Map Certifications to Recognised Standards
- Develop Certification Booklet
- Develop Certification Database
- Project roadblocks and issues

The detail of what was achieved at each of these stages of the project is shown below:

Project Initiation

The project was started in January 2007. While the final contracts were not signed until some time later, it was felt that, in order to complete the project in the desired time frame, work should begin immediately.

When the project started, the initial ideas were socialised with the designated APEC TEL project manager. After the approvals were obtained, the project went ahead.

Develop Project Methodology

The most important part of the project was to develop a framework whereby security skills certifications could be analysed and compared. This step in the process took a considerable amount of time because the project team were intent on ensuring that all skills certifications could be compared fairly and by using international standards already in place.

Research Certifications

At this stage of the project the team reviewed each certification syllabus and then populated the information gathered in a certification content spreadsheet. A difficult part of the comparison was that each organisation included different information about the certifications, thus making it hard to develop comparison information. At that time the team compiled additional certification information such as cost, experience requirements, ongoing certification maintenance requirements, duration of certification etc.

Once all of the information had been gathered an executive summary was written for each certification.

Develop Certification Database

Having gathered available and sufficient information regarding current certification programs, the list of certifications to be included was compiled. At this stage, a decision had to be made regarding the handling of vendor certifications. As these certifications are not intended to be "independent" (as their very value lies in the close integration with a specific product set), it was felt that these should be held and reported separately, without the same level of standards-compliance mapping as such information would provide a misleading representation of the Certificate's intent.

Requests for information were sent to APEC TEL Points of Contact (POCs) in order to obtain localised certification details from APEC economies. Unfortunately, while expectations were high of being able to include a range of APEC-region certifications, the results of the request for information were less than satisfactory. No responses were received from APEC economies.

Map Certifications to Recognised Standards

At this time it was necessary for the project team to select a body of knowledge through which the certifications could be compared. International standards were chosen due to their wide acceptance and broad awareness in both the information security and non-specialist communities. This selection would enable meaningful comparisons to be made between certifications and also the topics and areas that each certification covered could be mapped to the standard.

Certifications were mapped against two broad security framework documents to better capture the differences between the independent certifications, and provide a means for individuals and SMEs to find certifications closely tailored to their needs and areas of interest.

Mapping categories and tasks were extracted from the ISO IEC 17799:2005 Information Technology – Security Techniques – Code of Practice for Information Security Management document, and the FIPS 200 - Minimum Security Requirements for Federal Information and Information Systems document.

In addition to this mapping, independent certifications were mapped to a set of "security tasks" relevant to the industry. These included:

- Management of the Security
- Design Security Processes and Procedures
- Information Security Auditing
- Business Continuity Planning
- Implement Security Technologies
- Security Operations

Vendor or product-specific certifications were mapped to a set of security technologies to indicate their specific focus.

Develop Certification Booklet

An initial layout design was developed for the booklet to enable the certificates to be shown in an equal manner. This layout consisted of:

- A description of the certification
- The experience required
- The certification maintenance requirements

It also includes a mapping of the topics covered in the certification to:

- ISO/IEC 17799
- FIPS 200

Once all of the data had been gathered into a database of information it was processed into a booklet format. Any additional text content required to explain the process was developed as well. The document was then proof read for quality assurance.

Develop Certification Website

It is believed that the majority of users of the resources developed via this project will see this information via the web site. With this in mind the developers tried to ensure that the information was as accessible as possible and that it could be viewed in several different formats.

A developer was chosen to build the web site and the supporting database query system that would provide the meaningful reports. It was agreed that we would use the look and feel of the existing APEC TEL web site in order to maintain some level of continuity across the home APEC TEL web site and this site with the APEC sponsored information on it.

Once all of the information was uploaded and the reporting process was completed, the website underwent usability and security testing.

Project Issues & Constraints

The first aspect of the project that caused concern was the lack of feedback from APEC TEL economies. However, in some ways this was a known issue prior to the requests being distributed for the following reasons

- APEC TEL Points of Contact are frequently receive requests for information, and the TEL is currently pursuing a very heavy work program.
- The information sought in this particular process is somewhat obscure and in many cases it would not have been easily accessible to the POCs.
- In this case, the information was gathered through other means, however, for future projects it is recommended that the APEC

TEL discuss how projects can best obtain highly technical information from APEC members if it is required.

A second issue that arose was the escalating cost of web development. In years past, simple information only web sites with static pages were adequate for most project information sites. With the increase in complexity of the information being delivered and the increase in sophistication of the viewers of the web site, these simple sites are no longer adequate. Projects being developed for the future would do well to keep this in mind. This project was able to produce its deliverables within the specified budget but the budgets will need to increase in the future.

- Projects must ensure that adequate budget is allocated for modern database driven and interactive web sites.

PROJECT OUTCOMES

The two main outcomes for the project were to be:

- The "APEC Information Security Skills Certification Guide" contained in booklet format.
- A web site containing this same information with a user friendly method of retrieval.

Each of these two outcomes has been comprehensively addressed and will be demonstrated in the following sections.

Booklet

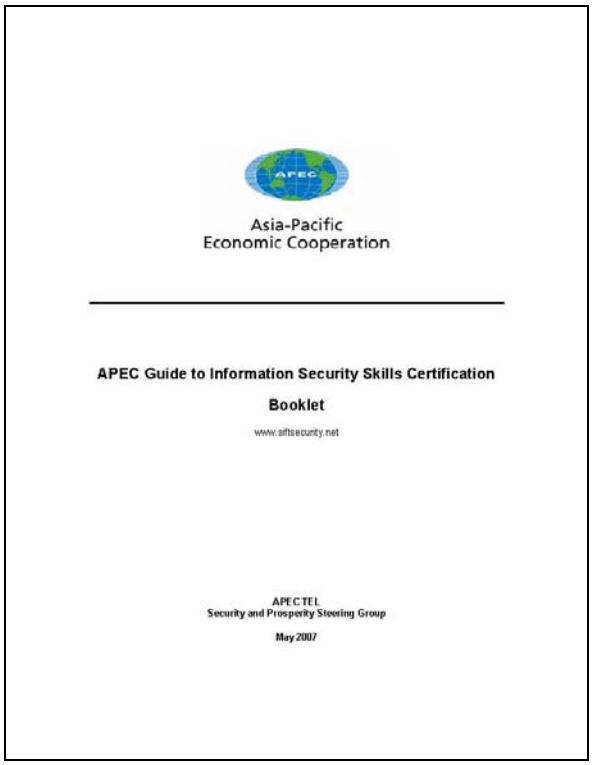
The booklet was developed with a simple design to enable the information that is contained on the web site to be taken away and printed for off-line reference. While the booklet cannot include the flexibility of the website in allowing case-by-case comparative analysis of certifications, there is sufficient information contained in the booklet to enable readers to make informed decisions.

The table of contents of the booklet is as follows:

- Introduction
- Information for Small-to-Medium Enterprises (SMEs)
- Information for Individuals
- Certification Categories
- Independent Certifications
- Appendix A1: ISO 17799 Security Tasks Mapping (CBCP – GCWN)
- Appendix A2: ISO 17799 Security Tasks Mapping (GISF – TICSA)
- Appendix B1: FIPS 200 Minimum Security Requirements Mapping (CBCP – GCWN)
- Appendix B2: FIPS 200 Minimum Security Requirements Mapping (GISF-TICSA)
- Appendix C: Vendor Certification Table
- Appendix D: Explanation of Certification Details
- Appendix E: How the certifications were mapped
- Appendix F: Validation of Certification Quality
- Appendix G: Other Links and Resources

Covering almost 100 pages it provides a significant amount of information about the types of certifications that are available to users and what they need to do to obtain them. It will also be helpful to employers who are confronted by employment applicants who indicate that they have these certifications.

Sample pages from the booklet are shown on the following pages.



Asia-Pacific
Economic Cooperation

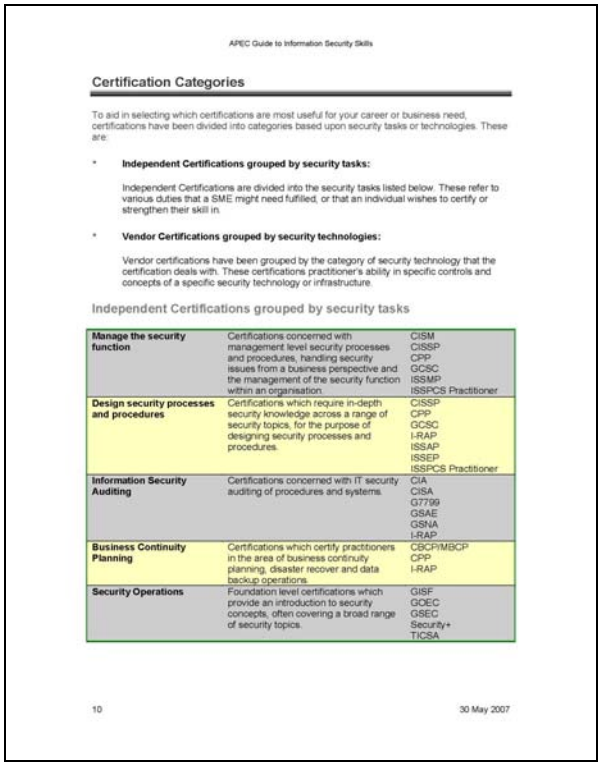
APEC Guide to Information Security Skills Certification Booklet

www.siftsecurity.net

APEC TEL
Security and Prosperity Steering Group

May 2007

Figure 1 Cover Page of the Booklet



APEC Guide to Information Security Skills

Certification Categories

To aid in selecting which certifications are most useful for your career or business need, certifications have been divided into categories based upon security tasks or technologies. These are:

* **Independent Certifications grouped by security tasks:**

  Independent Certifications are divided into the security tasks listed below. These refer to various duties that a SME might need fulfilled, or that an individual wishes to certify or strengthen their skill in.

* **Vendor Certifications grouped by security technologies:**

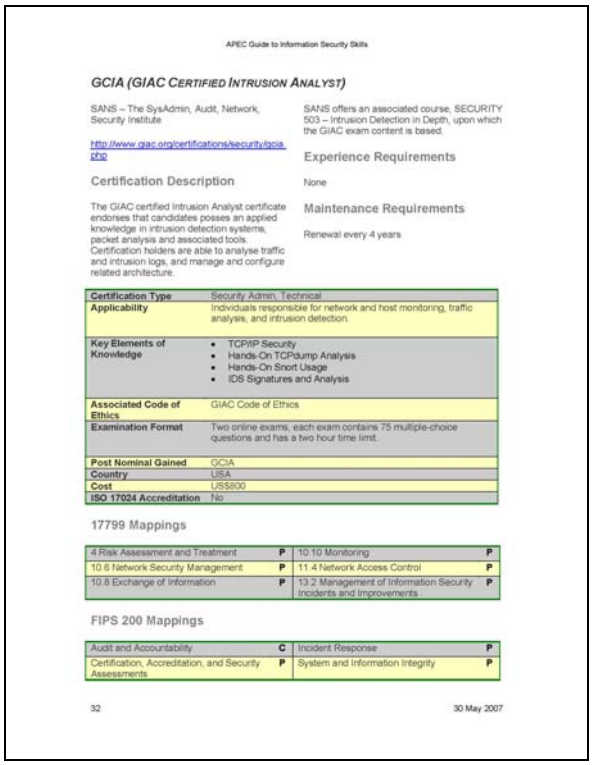
  Vendor certifications have been grouped by the category of security technology that the certification deals with. These certifications practitioner's ability in specific controls and concepts of a specific security technology or infrastructure.

Independent Certifications grouped by security tasks

Manage the security function	Certfications concerned with management level security processes and procedures, handling security issues from a business perspective and the management of the security function within an organisation.	CISM CISSP CPP GCSC ISSMP ISSPCS Practitioner
Design security processes and procedures	Certifications which require in-depth security knowledge across a range of security topics, for the purpose of designing security processes and procedures.	CISSP CPP GCSC I-RAP ISSAP ISSEP ISSPCS Practitioner
Information Security Auditing	Certifications concerned with IT security auditing of procedures and systems.	CIA CISA G7799 GSAE GSNA I-RAP
Business Continuity Planning	Certfications which certify practitioners in the area of business continuity planning, disaster recover and data backup operations.	CBCP/MBCP CPP I-RAP
Security Operations	Foundation level certifications which provide an introduction to security concepts, often covering a broad range of security topics.	GISF GOEC GSEC Security+ TICSA

10 30 May 2007

Figure 2 Page 10 Certification categories



APEC Guide to Information Security Skills

GCIA (GIAC CERTIFIED INTRUSION ANALYST)

SANS – The SysAdmin, Audit, Network, Security Institute

http://www.giac.org/certifications/security/gcia.php

SANS offers an associated course, SECURITY 503 – Intrusion Detection in Depth, upon which the GIAC exam content is based.

Experience Requirements

None

Certification Description

The GIAC certified Intrusion Analyst certificate endorses that candidates posses an applied knowledge in intrusion detection systems, packet analysis and associated tools. Certification holders are able to analyse traffic and intrusion logs, and manage and configure related architecture.

Maintenance Requirements

Renewal every 4 years

Certification Type	Security Admin, Technical
Applicability	Individuals responsible for network and host monitoring, traffic analysis, and intrusion detection.
Key Elements of Knowledge	• TCP/IP Security • Hands-On TCPdump Analysis • Hands-On Snort Usage • IDS Signatures and Analysis
Associated Code of Ethics	GIAC Code of Ethics
Examination Format	Two online exams, each exam contains 75 multiple-choice questions and has a two hour time limit.
Post Nominal Gained	GCIA
Country	USA
Cost	US$800
ISO 17024 Accreditation	No

17799 Mappings

4 Risk Assessment and Treatment	P	10.10 Monitoring	P
10.6 Network Security Management	P	11.4 Network Access Control	P
10.8 Exchange of Information	P	13.2 Management of Information Security Incidents and Improvements	P

FIPS 200 Mappings

Audit and Accountability	C	Incident Response	P
Certification, Accreditation, and Security Assessments	P	System and Information Integrity	P

32 30 May 2007

Figure 3 Sample Certification information page

Web Site

As mentioned, the web site is expected to be the entrance point for the majority of people seeking certification information.

Figure 4 Front page of the web site

The look and feel of the web site is based on the existing APEC TEL web site. The development of the look and feel resulted in a considerable overrun of time, as just as the site design had been completed, the APEC TEL web site was changed, thus forcing the graphic designer to re-do this part of the project in the new design.

The site has been set up to allow users to browse certificate by various tasks. The certifications focus on "vendor neutral" security strategies, systems and technologies and are provided by organisations with no vendor affiliation. They are divided into the security tasks listed below.

- Management of the Security Function Certifications concerned with management level security processes and procedures, handling security issues from a business perspective and the management of the security function within an organisation
- Design Security Processes and Procedures Certifications which require in-depth security knowledge across a range of security topics, for the purpose of designing security processes and procedures.
- Information Security Auditing Certifications concerned with IT security auditing of procedures and systems.
- Business Continuity Planning Certifications which certify professionals in the area of business continuity planning, disaster recover and data backup operations.
- Implement Security Technologies Certifications which cover security topics at an applied level, typically focused on a specific technology or knowledge area.
- Security Operations

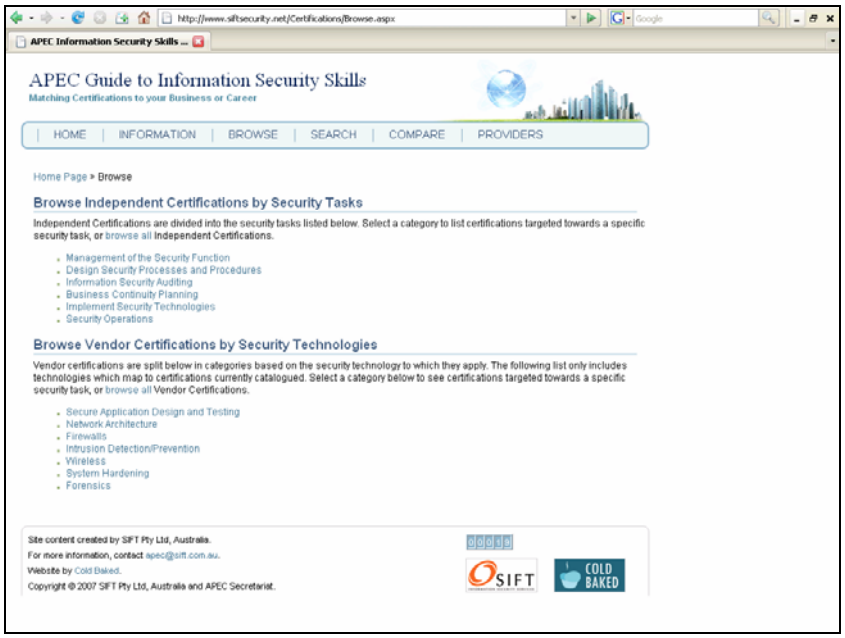


Figure 5 Browse Certifications Page

By selecting a task for review, a list of certifications relating to that task is shown. It is then possible to select any of the certifications shown in the list and a page showing information about that certification is shown.

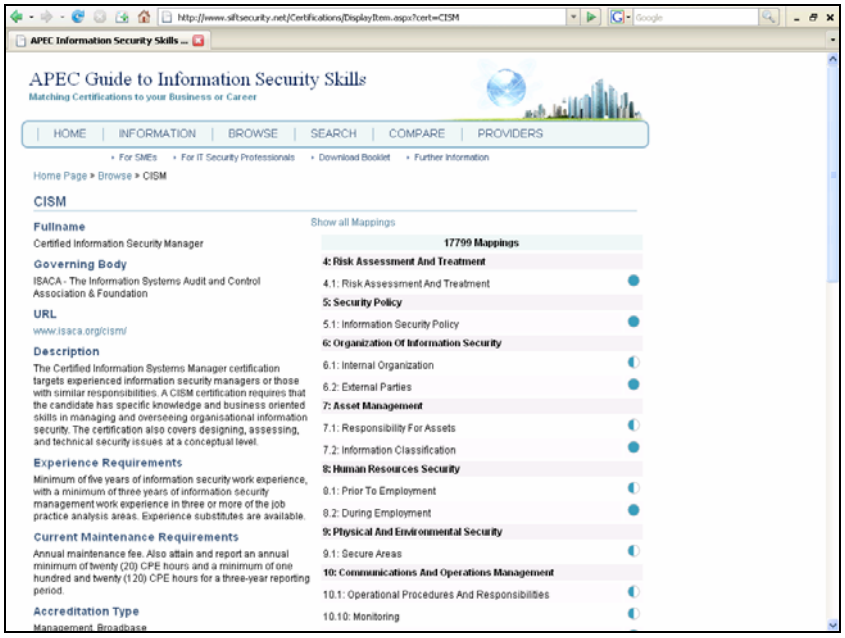


Figure 6 Sample Certification Page

The web site also allows the user to search certifications by the items in the International Standards that they cover. This will allow employers, information security professionals and students to seek certifications providing specific coverage of a section of the Standards.

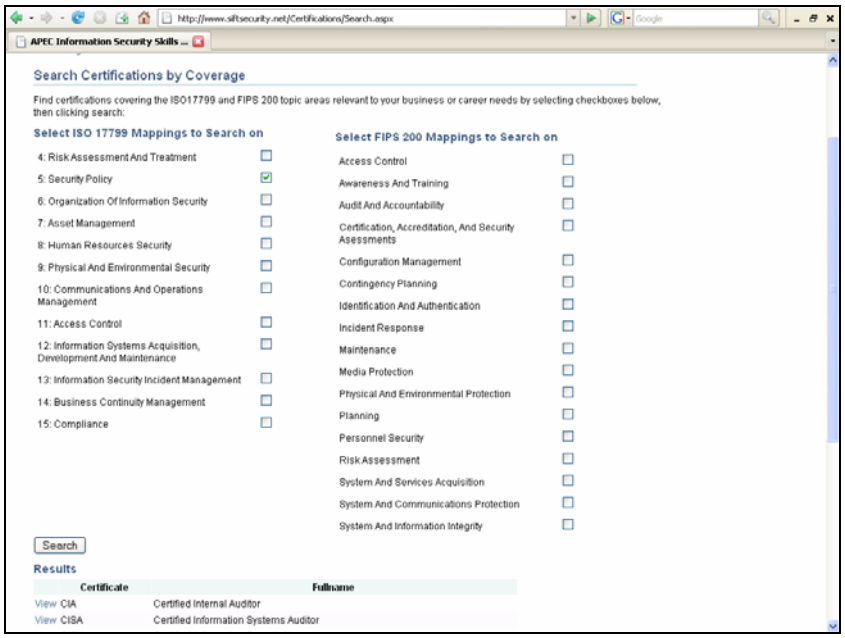


Figure 7 Search Certifications by Coverage

In addition, all certifications can be compared to allow a simple method of comparing certifications.

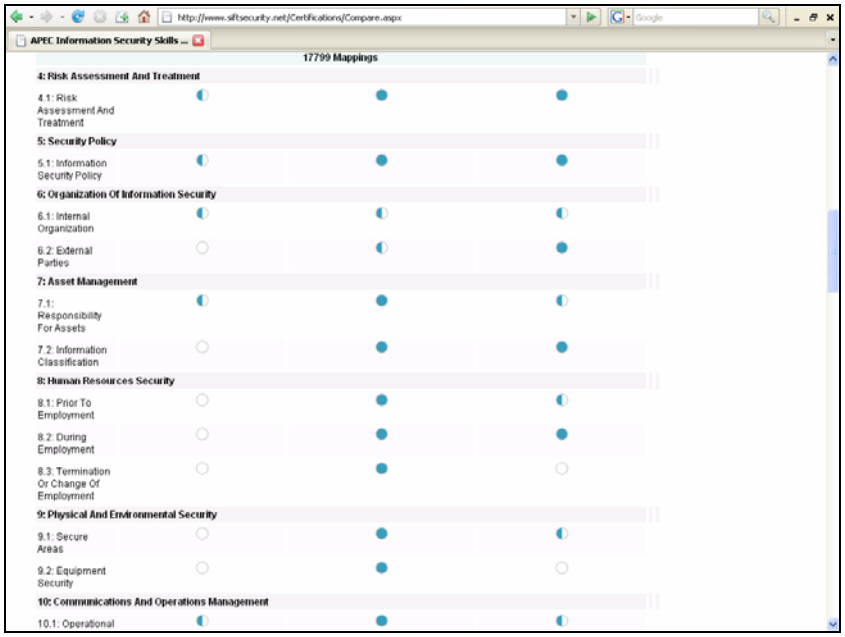


Figure 8 Compare Certifications

The last menu item allows certification organisations to add or change their details on the web site.

Web site hosting

At this time, the web site is hosted at www.siftsecurity.net, a domain made available for the hosting of this site over the next two (2) years by SIFT Pty Ltd for this purpose.

Given that the site uses the same look and feel as the APEC TEL web site, it may be easier to host the web site on the APEC TEL server, with a domain name specifically related to the project and/or to APEC TEL. This is recommended for discussion within the APEC TEL group.

RECOMMENDATIONS

Ongoing Project Support

As certifications content and requirements are frequently updated by providers, an ongoing support function is required. The scoped hosting and maintenance period for this website is 2 years. Ongoing support during this period will consist of the following actions:

- Certification details will be updated at the request of certification providers. It is beyond the scope of this project to constantly monitor and update certification details or to re-do the certification mappings, so changes will be limited to a per request basis and these requests will require sufficient detail to allow the change to be clearly identified.
- The website provides functionality for certification providers to add new certifications that were not included in the initial project. Certification details are to be entered by providers through the web interface, however these details will be reviewed and approved by SIFT staff before being displayed on the website.
- The website will be monitored by SIFT staff to ensure that it continues to function correctly and to ensure that ongoing administrative tasks, such as domain renewals, are performed. Analytics regarding use of the site will be monitored.

The amount budgeted for this item has not yet been funded.

It is expected that there are several ways to fund this final process

- APEC member economies could fund the process.
- Certification providers could fund the process. In return for this funding, they would be able to advertise on the web site.

APEC TEL SPSG may wish to discuss this process.

Summary of Issues for Discussion

Throughout this document some issues were raised for discussion at the APEC TEL. As the sponsoring steering group, the responsibility for these discussions would lie with the SPSG. The following points are a summary of the issues raised.

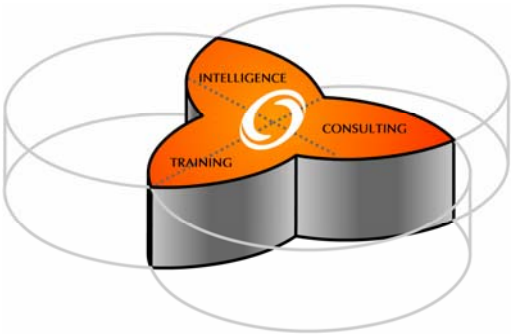
- To help future APEC TEL projects it is recommended that the APEC TEL discuss how projects can best obtain highly technical information from APEC members if it is required.
- Projects must ensure that adequate budget is allocated for modern database driven and interactive web sites.
- Ongoing funding of the Information Security Certification Assessment Guide web site can be achieved through

sponsorship or economy funding. The APEC TEL SPSG should discuss the best method

- Currently the Information Security Certification Assessment Guide web site is hosted at an address that is commercially oriented. APEC TEL SPSG may prefer to have it hosted as a subset of the APEC TEL web site. This issue should be discussed at APEC TEL36

SIFT PROFILE

About SIFT



Founded in 2000, SIFT is a leading Australian information security consulting, intelligence and training firm. We specialise in the delivery of independent advice, reviews and recommendations to the senior management of large, highly-regulated organisations.

Our focussed provision of information security advice and assurance services within the context of industry and country-specific regulatory requirements is unique. Our commitment to our clients is the ongoing delivery of concrete, specific and measured steps across the broad spectrum of information security body of knowledge.

SIFT has built long-term relationships with major clients and information security stakeholders in both the public and private sectors, providing exceptional customer focus throughout our business units. Through our security intelligence and industry & regulatory relationships, we are uniquely positioned to advise on information security within the Australian context.

Also realising the importance of information security in the wider community, SIFT is a sponsor of the Internet Industry Association (IIA) SME security portal, and provides pro-bono consulting services and financial support to The Inspire Foundation & Reachout! - a service that uses the Internet to provide much-needed information, assistance and referrals to young people going through tough times.

SIFT Services

Leveraging our unique perspective of information security issues in the Australian context, SIFT offers its clients a range of services:

Consulting

- Infrastructure & Application Penetration Testing
- Risk Assessment
- Information Security Governance, Compliance & Reporting
- Security Reviews, Audits and Benchmarking

Intelligence

- Policy & Procedure Development & Review
- Information Availability & Aggregation Reviews
- Custom Research Reports

Training

- Foundations of Information Security

- Foundations of Secure Web Application Design
- Industry Based Training
- Custom Training Programs

APEC Contact Details:
Monica Ochoa
APEC Secretariat,
35 Heng Mui Keng Terrace,
Singapore, 119616
Tel: (65) 6772 7661
Fax: (65) 6775 6013
mop@apec.org

APEC Publication Number:
APEC#207-TC-01.2

SIFT Pty Ltd

ABN 42 094 359 743
ACN 094 359 743

Head Office
Level 6, 62 Pitt Street
Sydney NSW 2000

Tel: + 61 2 9236 7276
Fax: + 61 2 9251 6393

Melbourne Office
Level 40, 140 William Street
Melbourne VIC 3000

Tel: + 61 3 9607 8274
Fax: + 61 2 9251 6393

To learn more visit
www.sift.com.au

For more information on this proposal please contact a SIFT Executive.

Nick Ellsmore
nick.ellsmore@sift.com.au
+61.414.519.510

Ashlee Ball
ashlee.ball@sift.com.au
+61.410.525.695

Michael Baker
michael.baker@sift.com.au
+61.417.823.971

Craig Searle
craig.searle@sift.com.au
+61.402.914.077