

# Building Synergy And Collaborating Towards Improving Security Standardization In Asia Pacific Region

## - Project Proposal And Discussion

**Mr Meng-Chow Kang, CISSP, CISA**

*Co-Chair, RAISS Forum*

*Chair, Security & Privacy Standards Technical Committee, ITSC, Singapore*

*Chief Security & Privacy Advisor, Asia Pacific Region, Microsoft*

### **ABSTRACT**

This paper is an attempt to bring forward the objectives of the Regional Asia Information Security Standards (RAISS) Forum into actionable projects whereby members of the Forum could build on the synergy of collaboration to improve security standards development, adoption, and use in the region. The focus of the RAISS Forum is deliberated, and three projects are proposed for considerations. The projects proposed include a security standards toolkit, an application security development standard, and a mutual recognition scheme for security certification programs in the region.

### **1. Introduction**

The Regional Asia Information Security Standards (RAISS) Forum is a regional gathering of information security standards experts, contributors, and organizations from around the Asia Pacific region with the objectives [2] of establishing a platform for standard bodies in Asia to discuss and share knowledge and experiences on issues relating to information security standards adoptions, developments, and other related activities. The Forum also provides a platform for identifying and developing security standards and other supporting activities at a regional level to fulfill the needs of Asia.

In order to achieve these objectives, specific actions need to be identified for execution by members and other interested experts in the subject matter of concerns. The areas of concerns need to be identified and prioritized so that the actions would bring about positive changes towards achieving the objectives.

This paper begins with a discussion on some of the possible areas of focus, which presents three specific areas of concerns whereby RAISS Forum, as a group, may be able to provide values to the regional economies as well as international standards organizations. To address these concerns, we propose three possible projects that may be undertaken.

## **2. Areas of Concerns**

### **2.1 Information Sharing and Dissemination**

One of the motivations leading to the organization of the RAISS Forum was the realization of the needs and importance of improving information sharing and communications between national bodies and security standards experts and professionals in the region. More critically, the dissemination of information relating to the current security standards development, status, and issues of concerns from ISO/IEC JTC 1/SC 27<sup>1</sup> (and other security standards related organizations, such as ITU-T<sup>2</sup>) to local interest groups and individuals is often constrained or slow. Reason being, not all economies are participating or observing members of the various international security standards organizations' meetings and workshops, and even when an economy has membership in the international standards organizations, there are often other resource challenges that constraint their regular participation, and subsequent local sharing. A number of emerging economies in the Asia region neither have formal organizations nor special interest groups from the industry established to keep tap of security standards developments and domestic promulgation and adoption. As a result, the benefits of security standards remain largely untapped in many such economies. In this regard, specific project(s) may be established to improve this situation, leveraging on the experiences and knowledge of experts from the more developed economies in the region.

### **2.2 Closing Gaps between Regional Needs and International Developments**

While there are many security standards that have been published by various standards organizations and within ISO/IEC JTC 1/SC 27 (or SC 27 in short), and roadmaps for the development of a new series of security standards are being established in the respective working groups in SC 27, their developments may not map directly to all the local or regional interest, requirements, and priorities. Where there are specific security standards that are deemed important to the regional economies but are not currently being addressed or

<sup>1</sup> ISO/IEC JTC 1/SC 27 - Sub-Committee 27, "Information Technology - Security Techniques", Joint Technical Committee 1 of International Organization for Standardization and International Electrotechnical Commission

<sup>2</sup> ITU-T - International Telecommunications Union - Telecommunication Standardization Sector

developed in the international standards arena, new projects may be initiated to develop such standards at the regional level before submitting to ISO or other standards organizations as new work items to become international standards. This approach could potentially reduce the timeframe required for a specification to be formalized and used within the region, and tap on the available expertise in the region in the development process. Practical experiences gained from its early adoption could also be incorporated into the regional specifications before submitting for international standardization.

### **2.3 Enhancing Assurance and Trust**

As observed from the inaugural meeting, economies like Japan, Singapore, and Chinese Taipei have implemented various security certification schemes on ISMS, mainly based on the BS 7799 Part 2 standard. Some of these implementations will eventually become internationally accredited and recognized certification scheme, when the ISO-equivalent of the underlying standards has been published. Singapore has also published a security standard on business continuity and disaster recovery for service providers (SS 507), and a local certification scheme based on this standard has been implemented. During the interim stages prior to attaining international recognition of a local certification scheme, companies, systems, and/or products that have been certified through the local certification scheme are not formally recognized by other economies. This interim period may take several years depending on the time taken for a local standard to become an international one.

On the other hand, the demands for trust and assurance through security certification are often from companies that are acquiring services from an external economy. For example, if a Japanese company outsources its disaster recovery services to a company in Singapore, the SS 507 security certification that the company in Singapore has been accredited locally will not be transparently recognized by the Japanese company and regulator. There is also no system or process available for the Japanese company to obtain information about the evaluation and accreditation performed in order to validate the certification to gain the assurance required, even if the Japanese company wishes to recognize the certification. The Japanese company will have to rely on all the information supplied by the company in Singapore to establish that trust, instead of an independent source. It appears that a system for mutual recognition of local certification schemes may be useful if it can be established to serve as interim systems to meet such requirements.

### 3. Proposed Projects

Focusing on the above mentioned challenges and opportunities, there are a number of projects that could potentially be developed for actions by members of the RAISS Forum. We propose three specific projects, one for each of the challenges identified. They are:

- Security Standards Toolkit,
- Application Security and Certification Framework, and
- Security Certification and Mutual Recognition.

The sub-sections below provide more details on each of these proposals.

#### 3.1 Security Standards Toolkit

A Security Standards Toolkit (SST) is proposed to address the concerns as highlighted in Section 2.1. This is to help emerging or developing economies to fast track the establishment of a security standards organization, and build capability and capacity to ensure local requirements are escalated, and new standards are promulgated and adopted.

The objectives of SST include the following:

1. Increase awareness and adoption of open standards relating to information security.
2. Provide understanding of SC 27 organization and standardization processes.  
Other standards organizations and related processes may also be included, depending on the contribution to this development.
3. Sharing of best practices in
  - a. Establishment of security standards organization;
  - b. Standards development and localization;
  - c. Participation and contribution to international and regional security standards organizations and groups;

- d. Common budgetary challenges and solutions;
  - e. Industry participation and contributions; and
  - f. Intellectual property protection.
4. Lay foundation for cross region standards adoption and mutual recognition of standards certification.
  5. Increase RAISS Forum membership by expanding the community of security standards professionals to contribute to standards development, and sharing of knowledge and best practices.

The following deliverables are proposed as part of this toolkit:

1. Contact List
  - a. List of security standards organizations and contact information, and
  - b. List of active contributors and contact information.
2. Documentation of existing knowledge and best practices
  - a. Guidance on regional and international security standards organizations and participations;
  - b. Guidance on planning and establishment of a local security standards body organization and membership;
  - c. Taxonomy of regional and international security standards; and
  - d. Applications of existing security standards, including development and adoption status of those standards, focusing on SC 27 (may also cover SC 17 (Cards & Personal Identification), SC 37 (Biometrics), and TC 68 (Financial Services Industry, including banking and securities).
3. Training material
  - a. Presentation slides on the above topics.
4. Delivery methods
  - a. Recorded and live Webcasts; and/or
  - b. Onsite seminars and workshops.

### 3.2 Application Security and Certification Framework

There are potentially many projects that may be developed to address the areas of concerns as discussed in Section 2.2. Our Thai colleague has in the second RAISS Forum meeting proposed the adaptation of the BS 7799 Lead Auditors training program for network and systems security administrators as a new guideline for improving the competency of these professionals. Such proposal is an important step for addressing some of the concerns discussed in Section 2.2, although the development of the guidelines may itself be another challenge.

In SC 27, there are various standards focusing on information security management, network security, cryptography, security protocols, as well as security assurance of products and technology (e.g., ISO/IEC 15408 series of standards on evaluation criteria for IT security). At the application layer, there are few initiatives that aim to address the security requirements. Attacks on web applications [4], such as SQL Injection [5] and Cross Site Scripting [3], are often made possible due to insecure development or coding practices, and the lack of a security focused development process when developing business applications. To manage security risk at the application layer, we need to consider the following:

1. Establish a consistent approach to application security, with a usable and well defined benchmark or standard for:
  - a. Application (code-level security), and
  - b. Process (that is repeatable, and with security deliverables and testing incorporated)
2. Provide security training for developers to improve secure application development practices, and
3. Create more awareness of the above to gain the buy-in of business management to encourage adoption and practices.

A project is therefore proposed to address these needs, to establish a framework encompassing a set of application security standards for common applications requirements, including a process to instill secure development practices, and a method (with criteria) for gaining security assurance of business applications and providers developing such applications.

### **3.2.1 Application Security Standard**

The application security standard should define a common set of security measures applicable for application layer security, and a base level of security against which applications will be assessed, therefore establishing the criteria for assurance purposes. The application security standard should be technology agnostic such that the recommendations can be implemented in a wide range of platforms, regardless of the underlying technology. Where specific technology needs to be addressed, the standard may reference other technology-specific guidance.

Assurance of compliance of the security standard should be based on source code examination and evaluation of base level security documentations identified in the standard.

### **3.2.2 Secure Development Process Standard**

The secure application development process standard should define a common set of secure development activities and provide a base process against which development lifecycles will be assessed. It should not mandate a specific development lifecycle or processes through defining common phases for structure, and provide references for lower level process-specific guidance as necessary. An example of a secure development process can be found in [1]. The content of this standard may include the following:

1. Security in the Requirements Phase
2. Security in the Design Phase
  - a. Threat Modelling
  - b. Security Education
3. Security in the Development Phase
  - a. Guidelines and Standards
  - b. Security Code Reviews
4. Security in the Testing Phase
5. Security in the Deployment and Support Phase

Assurance of practices in compliance with the secure development process standard may be based on stakeholder workshops, process documentation review, development project documentation review, and source code examination.

### **3.3 Security Certification and Mutual Recognition**

In Section 2.3, we deliberated the current issues relating to the variety of security certification schemes piloted and implemented in the Asia Pacific region, and the need by globalizing businesses to gain more trust and assurance of offshore suppliers of services and products, in particular, those operating outside of their home location. With the development of ISO/IEC 27001:2005 due to be published by the end of 2005, the assurance issue specific to ISMS<sup>3</sup> Certification (based on BS 7799-2 and other locally developed or customized security management system standard) may no longer be a major challenge. However, there remains other local standards that have yet to make it to ISO for international standardization, but have already been adopted for security certification purposes. Proposal such as the application security standard described in Section 3.2 may also fall into this category, if the region decided to adopt this approach for improving application layer security. A system, including related standards and guidelines, for mutual recognition of security certification within the region (initially amongst RAISS Forum members) may therefore be desired. This proposal is at its early stage and put forward in this paper mainly for soliciting more input and feedback, and assesses the level of interest amongst members of the RAISS Forum before a more structured proposal can be developed.

### **3.4 Development Plan**

The following high-level phases are outlined for development of the proposed projects.

1. Phase 0 - Formation of Working Group
2. Phase 1 - Feasibility Study
  - a. Develop justification paper
  - b. Develop detailed project plan

<sup>3</sup> Information Security Management System

- c. Draft budgetary requirements
  - d. Solicit supports from economies
  - e. Solicit funding from organization (e.g., ADBI, APEC, and Vendors)
3. Phase 2 - Development
- a. Develop documentation and training materials
  - b. Develop web portal for information sharing
  - c. Implementation planning
4. Phase 3 - Implementation
- a. Implement web portals
  - b. Invite and register participation
  - c. Conduct of onsite workshop and online Webcasts
  - d. Post-mortem
5. Phase 4 - Maintenance

### **3.5 Future Projects**

Given that SC 27 has a number of new security standards that are near their final publication stage, national bodies would need to evaluate their implications and suitable approach for adoption and implementation domestically. Projects along the line of preparing regional economies in these developments could potentially be beneficial to help the region to gain a head start in the adoption of new security standards, which in many instances, could be translated into competitive advantages for the industry.

## **4. Conclusion**

In order to achieve the objectives of the RAISS Forum, focused actions are required to address the issues that motivated the formation of the Forum. This paper has identified four areas of concerns, namely, readiness for information sharing and dissemination, gaps in existing standards and practices in application layer, mutual recognition of assurance certification, and preparing for emerging standards; and proposed three projects to be

initiated to address the first three concerns. To take the above initiatives forward, members of the RAISS Forum are requested to vote for and nominate representatives to form Working Group in order to bring the accepted proposals into its final deliverables. Members are also encouraged to provide detailed contributions (of knowledge) to specific project of interest, in any, to allow the Working Group to move forward more quickly in the development.

## 5. References

- [1] Howard, M. and Lipner, S. The Trustworthy Computing Security Development Lifecycle, MSDN Library, 2005  
<http://msdn.microsoft.com/security/default.aspx?pull=/library/en-us/dnsecure/html/sdl.asp>
- [2] Kang, M.C., Regional Asia Information Security Standards (RAISS) Forum - Terms of Reference in the Inaugural RAISS Forum Proceedings, (Tokyo, Japan, 2004), RAISS Forum, page 12-15  
[http://www.itsc.org.sg/standards\\_news/raiss/Preface%20to%20Article2.pdf](http://www.itsc.org.sg/standards_news/raiss/Preface%20to%20Article2.pdf)
- [3] Klein, A. Cross Site Scripting Explained, Sanctum, Inc., 2002, 10  
<http://crypto.stanford.edu/cs155/CSS.pdf>
- [4] Meier, J.D., Mackman, A., Dunner, M., Vasireddy, S., Escamilla, R. and Murukan, A. Building Secure ASP.NET Pages and Controls. in Finnel, L. ed. Improving Web Application Security: Threats and Countermeasures, Microsoft Press, 2003, 919  
<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetsec/html/THCMCh10.asp>
- [5] Spett, K. SQL Injection - Are your web applications vulnerable? SPI Dynamics, Inc., 2002, 25  
<http://www.spidynamics.com/whitepapers/WhitepaperSQLInjection.pdf>

Note: Biography of Meng-Chow Kang can be found in the **Preface** on page 05.

# Modified Risk Assessment Using A New Logical Way Of Thinking

**Dr Banchong Harangsri, Dr Komain Pibulyarajana,  
Ms Siriwan Apisiridej, Ms Doungkamol Suppitayakorn**

*Security Standard Research & Development  
Thai Computer Emergency Response Team (ThaiCERT)  
National Electronics and Computer Technology Centre (NECTEC), Thailand*

## ABSTRACT

This paper proposes to modify two courses targeting at managers auditors, and middle-to-higher management to include technical components so that they can be leveraged for training system and network administrators who play significant roles in information security within organizations.

## 1. Introduction

This proposal aims to modify two courses namely

- ISMS Auditor/Lead Auditor [1] and
- Practical Information Risk Management with ISO/IEC 17799/BS 7799 [2].

The first course is to train participants to become an ISMS lead auditor based on the BS 7799 standard [3] while the latter is to train participants to become an ISMS implementer, also based on the same standard. These two courses are targeted at managers, auditors in other fields, middle/high level managers, or even Chief Information Officers (CIOs), but not for system administrators (SA) and network administrators (NA).

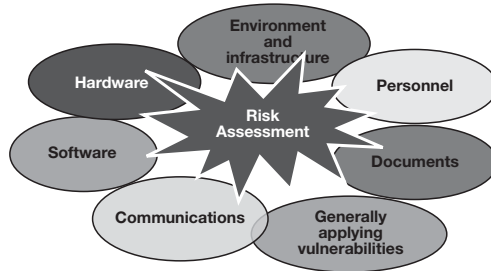
The modification proposed is to make the two original courses more suitable to the SAs and NAs. This is because it is realized that SA and NAs also play significant roles in the information security of an organization. The major modification plan will be in the part of Risk Assessment (RA) of the courses.

The original courses are assessed to be not appropriate for SAs and NAs and the reasons are:

- The technical personnel's (SAs and NAs) perspective usually differs from the management's perspective and their daily work concerning IT security is totally different.
- These courses do not provide an appropriate methodology for SAs and NAs to clarify the connections between the course material and their daily jobs.
- The RA provided by the courses focuses on too many type of risk (See the next section for more detail), and does not focus on much technicalities suited for the SAs and NAs.

## 2. RA in the Original Courses

The RA material provided categorize the types of threats (i.e., the threat taxonomy) into seven categories as shown in Figure 1, i.e., threats related to or affecting hardware, software, communications, generally applying vulnerabilities, documents, personnel, and environment and infrastructure, respectively.



**Figure 1:** Threat-Related Types in Original Courses

For example, for the threats related to 'Hardware', 'Software', and 'Environment', the threats and their vulnerabilities are shown in Table 1, Table 2, and Table 3 respectively.

Threats	Vulnerabilities
Deteriorations of storage media	Lack of period replacement schemes.
Power fluctuation	Susceptibility to voltage variations.
Extreme of temperature	Susceptibility to temperature variations.

**Table 1:** Examples of Threats and Vulnerabilities Related to Hardware

Threats	Vulnerabilities
S/W failure	Unclear or incomplete specification for developers.
Unreliable S/W	No or insufficient software testing.
Operational\staff error	Complicated user interface.

**Table 2:** Examples of Threats and Vulnerabilities Related to Software

Threats	Vulnerabilities
Theft	Inadequate or careless use of physical access control to buildings, rooms.
Physical Break-in	Lack of physical protection of the building doors and windows.
Power fluctuation	Unstable power grid.

**Table 3:** Examples of Threats and Vulnerabilities Related to Environment

### 3. Modified RA Approach

Such threat taxonomy provided by the original courses is assessed to be insufficient for SAs and NAs to apply to their system environment. We believe that a better threat taxonomy could be based on the tasks that they have to do daily. We call this approach 'task-oriented approach'. Our extensive experience on system and network security has shown that a preliminary version of the threat taxonomy could be shown in Table 4.

From Table 4, it is obvious that threat types are more relevant to their daily jobs as they are more logical and technically inclined for SAs and NAs to gain a good understanding and applicable to their workplace. The first layer in the Table shows the major threat types while the second layer shows the minor threats that are under the particular main types. For example, Access Control Requirement, User Registration, Privilege/Permission Management are under Access Control.

No.	Threat type (related to) Layer 1	Threat type (related to) Layer 2
1	Policy	
2	Documentation	
3.1	Physical Security	Physical Security Perimeter
3.2		Equipment Siting and Protection
3.3		Cabling Security
4.1	Operational Procedures and Responsibilities	Operational Change Control
4.2		Incident Management Procedures
4.3		Segregation of Duties
4.4		Role and Responsibilities
4.5		Operations
5	Information Back-up	
6	Unnecessary/Insecure Ports/ Services/Features/Packages	
7	Necessary/secure Ports/Services/ Features/Packages	
8	Basic System/Network Architecture	
9	Vulnerability/Patch	
10.1	Access Control	Access Control Requirement
10.2		User Registration
10.3		Privilege/Permission Management
10.4		Review of User Access Right
10.5		Password Use
10.6		Enforced Path
10.7		Segregation in Networks (Firewall)
10.8		Network Connection Control (Firewall)
10.9		Network Routing Controls
10.10		Terminal Log-on Procedures
10.11		User Identification and Authentication
10.12		Terminal Time-out
11.1	Monitoring System Access and Use	Event logging
11.2		Monitoring System Use
11.3		Clock Synchronization
12	Configuration Weakness	
13	Control Review	
14.1	Others (Standard and Well-known Threats)	Spoofing
14.2		Data Manipulation
14.3		Sniffing

**Table 4:** Threat Taxonomy (Task-Oriented)

To demonstrate the approach, we will use an example here. The firewall checklist below has been taken from the web site:

**[http://www.principlelogic.com/docs/Firewall\\_Best\\_Practices.pdf](http://www.principlelogic.com/docs/Firewall_Best_Practices.pdf)**

which is aimed to harden a firewall. Each item in the list is what SAs/NAs have to do to secure their firewall. On the contrary, if any of the items are not implemented, then it becomes a vulnerability to the system. For example, if the item 'Deny all traffic by default and only enable those services that are needed' is not looked upon, then some unauthorized traffic could pass through the firewall, possibly leading to an attack. Therefore all items in the checklist are a vulnerability list if we don't do them.

- Deny all traffic by default and only enable those services that are needed.
- Disable or uninstall any unnecessary services and software on the firewall that are not specifically required.
- Limit the number of applications that run on the firewall in order to let the firewall do what it's best at doing. Consider running anti-virus, content filtering, VPN, DHCP, and authentication software on other dedicated systems behind the firewall.
- If possible, run the firewall service as a unique user ID instead of administrator or root.
- Change the default firewall administrator or root password. The password should not be found in a dictionary, and at a minimum, should be 8 characters long using a combination of uppercase and lowercase letters, numbers, and other characters such as \$, %, and @, and needs to be changed frequently.
- Do not rely on packet filtering alone. Use stateful inspection and application proxies if possible.
- Ensure that you're filtering packets for correct addresses based upon the SANS Top 20 Vulnerabilities List section titled Not filtering packets for correct incoming and outgoing addresses found at <http://www.sans.org/top20.htm>
- Ensure that you're filtering or disabling all unnecessary ports and common vulnerable ports based upon the SANS Top 20 Vulnerabilities List sections titled Large number of open ports and Common Vulnerable Ports found at <http://www.sans.org/top20.htm>
- If a malicious user can obtain physical access to the firewall, anything can happen. Ensure that physical access to the firewall is controlled.

- A lot of times, firewalls are doing less (or more) than what they should be doing based on your business needs and information flow requirements. Keep your firewall configuration as simple as possible and eliminate unneeded or redundant rules to ensure that the firewall is configured to support your specific needs.
- Make sure the security rule set on the firewall remains consistent with the organization's written information security policy. You do have a security policy, don't you?
- Consider using the following in conjunction with a firewall:
  - Network-based intrusion detection system (IDS)
  - Hosted-based personal firewall/intrusion prevention products to protect workstations and servers from malicious traffic coming in over the allowed ports on the firewall
  - Anti-virus software that is regularly updated
  - E-mail and web content filtering software
  - URL filtering software
  - Third-party authentication systems
- If possible, use a firewall in conjunction with a router when connecting to the Internet to help prevent denial of service attacks and successful penetrations.
- Patch the firewall's operating system and application software with the latest code on a regular basis. However, make sure you test these updates in a controlled, non-production environment whenever possible.
- Use firewalls internally to segment networks and permit access control based upon business needs.
- Enable firewall logging and alerting if possible.
- Use a secure remote syslog server that makes log modification and manipulation more difficult for a malicious user.
- Regularly monitor the firewall logs. Treat the logs as business records and include them in your data retention policy.
- Note any firewall log entries that don't look right and investigate them immediately.
- Periodically backup the firewall logs (preferably onto write-once media such as CD-R) and store for future reference and/or legal protection in the case of an intrusion that must be investigated.
- Use change-management practices for the firewall to approve changes needed, assess the reason(s) for the changes, document the changes made, and describe the necessary back-out procedures in case the changes fail.

- Perform vulnerability assessments on your firewall on an ongoing basis to test for known software flaws and weaknesses. New exploits are continuously discovered and must be tested for on a consistent basis. In addition, the slightest firewall system or rule set modifications can completely change the firewall's security capabilities. Perform these tests on every interface of the firewall in all directions. Also, perform these tests with and without the firewall rules enabled to determine how vulnerable you will be when the firewall is not functioning properly.
- Perform ongoing audits, at least yearly, on the firewall to compare what you say you're doing in your security policy with what's actually being done and to ensure adherence to any government regulations that pertain to your organization.
- Require that users run anti-virus and personal firewall/intrusion prevention software on all remote computers. This will help prevent malicious code or an attacker from penetrating the corporate network in the event that the remote computer is compromised. Make this something that cannot be easily disabled. No exceptions.
- Constantly monitor (or subscribe to) your firewall vendor's security bulletins.
- Regularly backup the firewall configuration files, and keep the backups offsite.
- Firewalls can be easily circumvented if using wireless network systems internally. Again, use personal firewalls/intrusion prevention software on all internal hosts whenever possible.
- Remember that firewalls won't prevent attacks that originate from inside your network. An acceptable usage policy, personal firewalls/intrusion prevention software, network monitoring, content filtering, and access controls on all hosts can help lower these risks.

Categorization is then carried out for each of the vulnerabilities in the list under its minor threat types. For example, 'Deny all traffic by default and only enable those services that are needed' could be categorized under 'policy' threat type. 'Disable or uninstall any unnecessary services and software on the firewall that are not specifically required' could be categorized under 'Unnecessary/Insecure Ports/Services/Features/Packages'. Working through such a list, we get the result as shown in Table 5.

No.	Threat (Task-Oriented) Layer 1	Threat (Task-Oriented) Layer 2	Vulnerability (Checklist)
1	Policy		<ul style="list-style-type: none"> <li>- Deny all traffic by default and only enable those services that are needed.</li> <li>- Disable or uninstall any unnecessary services and software on the firewall that are not specifically required.</li> <li>- Ensure that you're filtering packets for correct addresses based upon the SANS Top 20 Vulnerabilities List section titled <i>Not filtering packets for correct incoming and outgoing addresses</i> found at <a href="http://www.sans.org/top20.htm">http://www.sans.org/top20.htm</a></li> </ul>
2	Documentation		Use change-management practices for the firewall to approve changes needed, assess the reason(s) for the changes, document the changes made, and describe the necessary back-out procedures in case the changes fail.
3	Physical Security	Physical Security Perimeter	If a malicious user can obtain physical access to the firewall, anything can happen. Ensure that physical access to the firewall is controlled.
		Equipment Siting and Protection	
		Cabling Security	
	Operational Procedures and Responsibilities	Operational Change Control	
		Incident Management Procedures	Note any firewall log entries that don't look right and investigate them immediately.
		Segregation of Duties	
		Role and Responsibilities	
		Operations	
	Information Back-up		<ul style="list-style-type: none"> <li>- Periodically backup the firewall logs (preferably onto write-once media such as CD-R) and store for future reference and/or legal protection in the case of an intrusion that must be investigated.</li> <li>- Regularly backup the firewall configuration files, and keep the backups offsite.</li> </ul>

**Table 5:** An Example of Threats and Vulnerabilities Analysis for a Firewall

No.	Threat (Task-Oriented) Layer 1	Threat (Task-Oriented) Layer 2	Vulnerability (Checklist)
	Unnecessary/ Insecure Ports/ Services/Features /Packages		<ul style="list-style-type: none"> <li>- Limit the number of applications that run on the firewall in order to let the firewall do what it's best at doing. Consider running anti-virus, content filtering, VPN, DHCP, and authentication software on other dedicated systems behind the firewall.</li> <li>- Ensure that you're filtering or disabling all unnecessary ports and common vulnerable ports based upon the SANS Top 20 Vulnerabilities List sections titled <i>Large number of open ports and Common Vulnerable Ports</i> found at <a href="http://www.sans.org/top20.htm">http://www.sans.org/top20.htm</a></li> </ul>
	Necessary/secure Ports/Services/ Features/ Packages		
	Basic System/ Network Architecture		<ul style="list-style-type: none"> <li>- If possible, use a firewall in conjunction with a router when connecting to the Internet to help prevent denial of service attacks and successful penetrations.</li> <li>- Consider using the following in conjunction with a firewall: <ul style="list-style-type: none"> <li>• Network-based intrusion detection system (IDS)</li> <li>• Hosted-based personal firewall/intrusion prevention products to protect workstations and servers from malicious traffic coming in over the allowed ports on the firewall</li> <li>• Anti-virus software that is regularly updated</li> <li>• E-mail and web content filtering software</li> <li>• URL filtering software</li> <li>• Third-party authentication systems</li> </ul> </li> <li>- Do not rely on packet filtering alone. Use stateful inspection and application proxies if possible.</li> <li>- Require that users run anti-virus and personal firewall/intrusion prevention software on all remote computers. This will help prevent malicious code or an attacker from penetrating the corporate network in the event that the remote computer is compromised. Make this something that cannot be easily disabled. <u>No exceptions.</u></li> </ul>

**Table 5:** An Example of Threats and Vulnerabilities Analysis for a Firewall (cont'd)

No.	Threat (Task-Oriented) Layer 1	Threat (Task-Oriented) Layer 2	Vulnerability (Checklist)
			<ul style="list-style-type: none"> <li>- Firewalls can be easily circumvented if using wireless network systems internally. Again, use personal firewalls/intrusion prevention software on all internal hosts whenever possible.</li> <li>- Remember that firewalls won't prevent attacks that originate from inside your network. An acceptable usage policy, personal firewalls/intrusion prevention software, network monitoring, content filtering, and access controls on all hosts can help lower these risks.</li> </ul>
	Vulnerability/ Patch		<ul style="list-style-type: none"> <li>- Patch the firewall's operating system and application software with the latest code on a regular basis. However, make sure you test these updates in a controlled, non-production environment whenever possible.</li> <li>- Perform vulnerability assessments on your firewall on an ongoing basis to test for known software flaws and weaknesses. New exploits are continuously discovered and must be tested for on a consistent basis. In addition, the slightest firewall system or rule set modifications can completely change the firewall's security capabilities. Perform these tests on <u>every</u> interface of the firewall in <u>all</u> directions. Also, perform these tests <u>with</u> and <u>without</u> the firewall rules enabled to determine how vulnerable you will be when the firewall is not functioning properly.</li> <li>- Constantly monitor (or subscribe to) your firewall vendor's security bulletins.</li> </ul>
	Access Control	Access Control Requirement	A lot of times, firewalls are doing less (or more) than what they should be doing based on your business needs and information flow requirements. Keep your firewall configuration as simple as possible and eliminate unneeded or redundant rules to ensure that the firewall is configured to support your specific needs.
		User Registration	
		Privilege/ Permission Management	If possible, run the firewall service as a unique user ID instead of administrator or root.
		User Password Management	

**Table 5:** An Example of Threats and Vulnerabilities Analysis for a Firewall (cont'd)

No.	Threat (Task-Oriented) Layer 1	Threat (Task-Oriented) Layer 2	Vulnerability (Checklist)
		Review of User Access Right	
		Password Use	Change the default firewall administrator or root password. The password should not be found in a dictionary, and at a minimum, should be 8 characters long using a combination of uppercase and lowercase letters, numbers, and other characters such as \$, %, and @, and needs to be changed frequently.
		Enforced Path	
		Segregation in Networks (Firewall)	Use firewalls internally to segment networks and permit access control based upon business needs.
		Network Connection Control (Firewall)	
		Network Routing Controls	
		Terminal Log-on Procedures	
		User Identification and Authentication	
		Terminal Time-out	
	Monitoring System Access and Use	Event logging	Enable firewall logging and alerting if possible.
		Monitoring System Use	<ul style="list-style-type: none"> <li>- Regularly monitor the firewall logs. Treat the logs as business records and include them in your data retention policy.</li> <li>- Note any firewall log entries that don't look right and investigate them immediately.</li> </ul>
		Clock Synchronization	
	Configuration Weakness		
	Control Review		<ul style="list-style-type: none"> <li>- Make sure the security rule set on the firewall remains consistent with the organization's written information security policy.</li> <li>- Perform ongoing audits, at least yearly, on the firewall to compare what you say you're doing in your security policy with what's actually being done and to ensure adherence to any government regulations that pertain to your organization.</li> </ul>

**Table 5:** An Example of Threats and Vulnerabilities Analysis for a Firewall (cont'd)

No.	Threat (Task-Oriented) Layer 1	Threat (Task-Oriented) Layer 2	Vulnerability (Checklist)
	Others (Standard and Well-known Threats)	Spoofing	
		Sniffing	Use a secure remote syslog server that makes log modification and manipulation more difficult for a malicious user.

**Table 5:** An Example of Threats and Vulnerabilities Analysis for a Firewall (cont'd)

#### 4. Procedure to Apply our RA Approach

With such a threat and vulnerability analysis as shown in Table 5, we need to define appropriate controls for the vulnerabilities.

Therefore, the whole procedure to apply our RA approach step by step is as follows:

1. Select an important asset - say a firewall, that requires protection.
2. Find out a number of checklists (vulnerabilities) for the asset - usually through searching from the Internet.
3. Put each item in the checklist under its threat type.
4. Repeat step 3 until completing all items in the checklist.
5. Calculate risks of each item (vulnerability) in the threat tree by using the formula;  
Risk value = asset value x threat level x vulnerability level x the probability that the threat will make use of the vulnerability.
6. Sort all the risks in ascending order.
7. Select to address some of the risks with an unacceptably high value.
8. Select the appropriate controls for those selected risks where the controls could be found from the BS 7799 standard.

## 5. **Benefits of the Proposed Approach**

The benefits of the proposed approach include the following:

- As compared with the current approach, the proposed approach is more logical for SAs and NAs or technical personnel to think of threats from their daily jobs. Checklists (threats/vulnerabilities) that are relevant to their jobs, such as firewall, router checklists and so on could be found on the Internet.
- The more checklists for a particular system/network device they have, the more threats and vulnerabilities they will be able to cover and that would translate into higher security assurance for the systems/devices that they are managing.
- When SAs and NAs have gone through the procedure a few times with a number of assets, the taxonomy for the assets will be applicable to and reusable by other assets to consider in the future. For example, the checklist item (vulnerability) for the firewall 'Disable or uninstall any unnecessary services and software on the firewall that are not specifically required' could be applied to a router as its vulnerability.

## 6. **Major Course Modification and Collaboration Needed**

The following are proposed to be carried out for the course modification:

- Provide a new material with guiding examples/concepts especially on RA using the new threat taxonomy provided here.
- Provide a new workshop on RA to practice/sharpen the skills of the participants.

As this work is still in the infancy stage, we would like to seek for network and server security specialists to help develop the material for the course.

## 7. References

- [1] ISMS Auditor/Lead Auditor, RWTUV
- [2] Practical Information Risk Management with ISO/IEC 17799/BS 7799, Training Partners
- [3] BS 7799-2:2002 standard - Information security management system (ISMS) - Requirements

Note: Biographies of the authors can be found in the paper **"Thailand Status Update On IT Security Standards And Implementation"** on page 66 and 67.