The Simple Information Security Audit Process: SISAP

Bel G. Raggad, Ph.D.

Ivan G. Seidenberg School of Computer Science
and Information Systems
Pace University
Pleasantville, NY 10570

Emilio Collar, Jr., PhD.

Ancell School of Business
Western Connecticut State University
Danbury, CT 06810

Summary

The SISAP (Simple Information Security Audit Process) is a dynamic security audit methodology fully compliant with the ISO 17799 and BS 7799.2, and conformant with the ISO 14508 in terms of its functionality guidelines. The SISAP employs a simulation-based rule base generator that balances risks and business value generation capabilities using the Plan-Do-Check-Act cycle imposed in BS 7799.2. The SISAP employs a concept proof approach based on 10 information security best practices investigation sections, 36 information security objectives, and 127 information security requirements, as specified in the ISO 17799. The auditor may apply, for collecting, analyzing, and fusing audit evidence obtained at various audit steps, selected analytical models like certainty factors, probabilities, fuzzy sets, and basic belief assignments. The SISAP adopts fully automated elicitation worksheets, as in SASA (Standard Analytic Security Audit), COBRA, and others.

Keywords

Security audit, vulnerability assessment, threats, ISO 17799, nominal audit, risk assessment

1. Introduction

Security in any system should be valued in terms of its risks. However, the process to determine which security controls are appropriate and cost-effective is quite often a complex and subjective matter. Risk Analysis is an essential component in securing the target company, and thus allowing the risk to be managed effectively. Adequately securing the company cannot, however, be achieved without a thorough IS security audit, similar to the one for which we design the SISAP methodology [10].

An information security audit approach should identify the potential business impacts of unavailability, loss of integrity, and breach of confidentiality, as well as the value of the business assets ([2], [3], [9]). The impacts identified in the risk analysis are then used to determine which areas and issues should be considered further. This condition is extremely important, as it is used later in the security audit project to justify recommendations and conclusions.

The SISAP evaluates the company's compliance to baseline security and control standards that have been defined in corporate security policy and laws and regulations. While external security audit is not often accepted in detailed system and application audits, it may be of great importance in a security management review. The SISAP auditor establishes that the network control environment and administrative practices meet a predetermined and commercially-acceptable level of compliance. This explains why external auditors who are familiar with more diversified computing and networking environments can add value to the security review being discussed.

The main goal of a security audit is to ascertain an organization's ISMS (Information Security Management System) compliance with both the security control structure defined by the ISO 17799 and the planning, analysis, design, implementation, and maintenance conditions defined in BS 7799.2 [1]. The security audit is further separated into four grades:

Grade 1: Internal audit for self compliance
Grade 2: External audit for an independent compliance
Grade 3: Certification by a certifier
Grade 4: Accreditation of a certifier

A company may seek to achieve compliance with ISO 17799, or even BS 7799-2, based on a simple but acceptable self-assessment. The ISO 17799 does not require any process by which the

standard is implemented [1]. As soon as the organization implements the information security best practices defined in ISO 17799, it can declare itself compliant with this standard. Even though this is obviously a very important step towards better information security, this assessment still has to be verified by an independent auditor. A more essential step should next be a grade 2 security audit conducted by an external auditor, or a grade 3 security audit with certification.

An organization seeking to achieve certification for ISO 17799 must engage a certification body to conduct the audit project. The size of the audit effort will obviously depend on the size and complexity of the system being audited, as well as any special domain knowledge requirements.

The simple information security audit process (SISAP) is an information system security audit methodology that complies with both ISO 17799, and BS 7799.2. The conformity with ISO 15408 is also present at the functionality level. It simply looks for violations of the corporate security policy and recommends feasible corrections that reduce the corporate security risk position to a tolerated level prescribed in the security policy and still acceptable by information owners. The SISAP consists of the following phases: 1. Security Audit Planning; 2. Review of Policy; 3. Nominal Audit; 4. Technical Audit; 5. Data Analysis; 6. Risk Analysis; 7. Report; and 8. Post-Audit. These are the same steps found in any other security audit methodology reported in the literature ([2], [3]). The contents of steps is however very unique to the SISAP methodology.

The preparation effort constitutes the planning of the security audit project and the review of the corporate security policy. These two steps are intentionally left out of this article as they may be designed in any way the auditors desire without affecting the working of the rest of the SISAP methodology. The last three steps are also left for the auditors to design. The SISAP does not impose any risk methodology, as long as it is consistently adopted and well defined in the corporate security policy. The article will then limits the presentation of the SISAP methodology to two phases: 1) the nominal security audit effort, and 2) the technical security audit effort.

2. The SISAP Nominal Audit

The nominal audit phase consists of three objectives:

1. Assess to what extent is the company that is target of the audit (TOTA) compliant with the ISO 17799;
2. Compute an estimate for the current TOTA's security posture in terms of its conformity to the best practices defined in the ISO 17799;
3. Produce a list of claims in various security best practices sections defined in the ISO 17799 that will serve in defining the scope of the technical security audit phase.

A security audit, of any grade, consists however of documentation review in which the auditor reviews the security posture of the company in terms of the best security practices defined in ISO 17799. The auditor is faced with a large number of information assets constituting the company's computing environment.

Even though the ISO 17799 does not impose any process to verify that the organization's satisfaction of the best security practices defined by the standard, this article adopts an outcome-based security audit process. Such a security audit process, in addition to the verification that the best security practices are implemented by the organization, also makes sure that those practices are actually working and yielding the security posture prescribed in the corporate security policy.

The SISAP also includes detailed and comprehensive testing procedures to support the vague findings and guidelines produced in security management, as defined in IS 17799. These guidelines are very useful in defining the scope of the nominal audit part of the SISAP in terms of the following 10 information security investigation sections: 1) Policy; 2) Organisation; 3) Controls; 4) Personnel; 5) Physical; 6) Communications; 7) Access; 8) Development; 9) Continuity; and 10) Compliance. These are the 10 security areas described in sections 3 to 12 in the ISO 17799 document.

The nominal audit investigates the TOTA's compliance with the ISO 17799 as depicted in Figure 1. This investigation will estimate the

TOTA's security posture and produces the list of claims that includes the list of information assets and vulnerabilities that define the scope of the testing activities constituting the technical security audit phase of the SISAP. The claims contain the approved prescriptions for the technical audit testing activities. Since BS 7799.2 requires a risk-driven security program at the output of the security audit to constitute the auditors-approved specifications for the design of the TOTA's ISMS. The framework defining the nominal security audit steps are depicted in Figure 2.

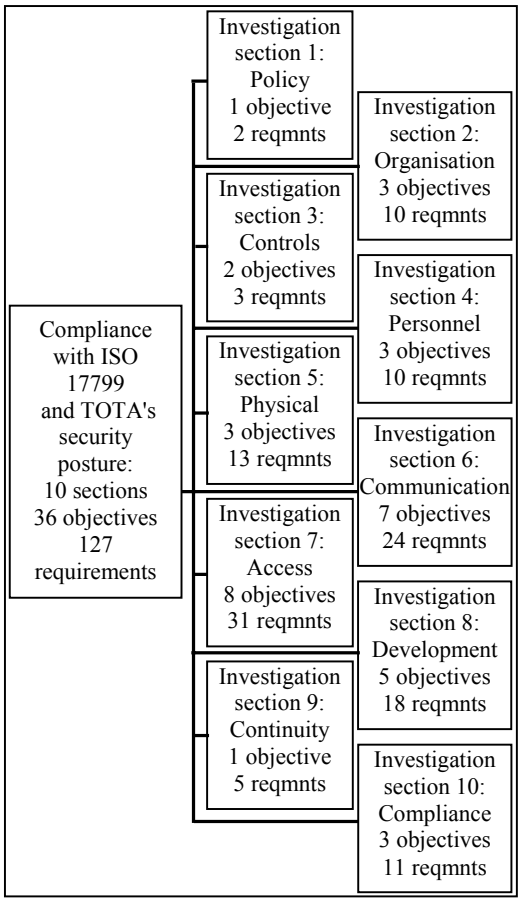

Figure 1: TOTA's compliance with ISO 17799

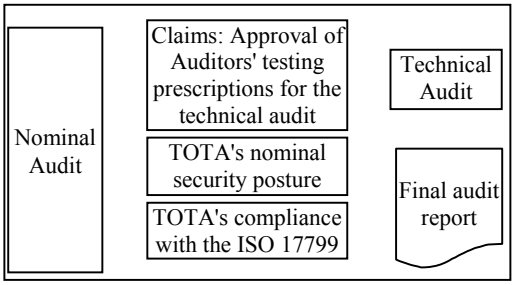

Figure 2: Framework for the nominal security

The SISAP employs a concept proof approach based on 10 information security best practices investigation sections, 36 information security objectives, and 127 information security requirements, as specified in the ISO 17799. The nominal audit adopts a concept proof scheme, as depicted in Figure 3. This schema expresses that in order to verify the TOTA's compliance with the best practices (called the C concepts) defined in section s, s=1,10, all security objectives (called the B concepts) defining s should be satisfied, and in order to satisfy these security objectives, all the respective information security requirements (called the A concepts) have to be satisfied.

Given the concept proof structure, shown in Figure 3, and rule structure used in the nominal security audit, the TOTA's nominal security posture may be computed, as in rule base systems, in different ways, using the certainty factor algebra, probabilistic computing, or fuzzy set theory. This article will however simply use the average of scores the auditors attribute to different concepts in computing the nominal security postures. For example, a simple 5-point scale may be used to investigate the TOTA's compliance with the ISO 17799 (1:the requirement/objective or best practice is non-existing; 2: poor; 3: moderate; 4:acceptable, full compliant with). That is, in this case, compliance is met whenever the concept C obtains a score equal or higher than 2.5. The security posture is estimated using the average score over the 10 investigation sections for which the concepts C1 through C10 are nominally evaluated.

3. The ABC concept structure in the SISAP

The SISAP is a dynamic security audit approach based on both the ISO 17799 and BS 7799.2. A security standard is regarded as a control system where an iterative control mechanism simulates standard compliance inputs to produce an ISMS design that translates the initial security audit objectives. While the ISO 17799 presents a framework that provides best practices for information security management, the BS 7799-2 specifies how an ISMS is developed and maintained in order to make operational the controls in ISO 17799.

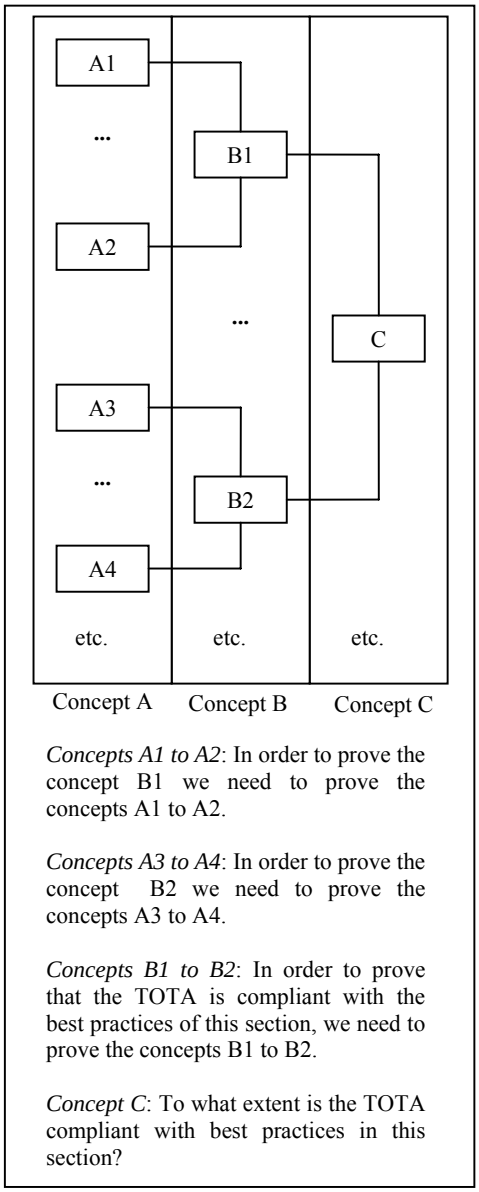

Figure 3: Concept proof scheme adopted in the nominal audit phase

The SISAP imposes a PDCA cycle, as indicated in BS 7799.2. The PDCA cycle is written in terms of risk identification, assessment, management, and cost-effective security (RIAMS). The statement of applicability of the security audit will contain a risk-driven security program, based on RIANS steps, that explains how selected security controls mitigate risks to achieve an acceptable risk position as specified in the corporate security policy.

The SISAP regards the ISO 17799 as a dynamic simulation-based rule base generator capable of devising an acceptable operational security control system that serves as a groundwork for an effective ISMS. The ISO 17799 ABC structure is defined as (C[m](B[n](A[k]))), where A is the auditor's evaluations, B compliance with security objectives, and C compliance with security best practices; that is, m=10, n=36, k=127. Figure 1 depicts the general framework of analysis of the ISO 17799. This may be implemented as a fuzzy expert system, a crisp or probabilistic rule base, or a simple crisp decision table. The simulation-based rule base generator used in the SISAP is depicted in Figure 4. The SISAP structures the ISO 17799 as follows:

(C1[1](B1[1:2](A1[2])))
(C2[1](B2[3:7,2,1](A2[10])))
(C3[1](B3[2:1,2](A3[3])))
(C4[1](B4[3:4,1,5](A4[10])))
(C5[1](B5[3:5,6,2](A5[13])))
(C6[1](B6[7:6,2,1,3,1,4,7](A6[24])))
(C7[1](B7[8:1,4,2,9,8,2,3,2](A7[31])))
(C8[1](B8[5:1,4,5,3,5](A8[18])))
(C9[1](B9[1:5](A9[5])))
(C10[1](B10[3:7,2,2](A10[11])))

The meaning of (C1[1](B1[1:2](A1[2]))) is that the first investigation section consists of one security objective expressed in terms of 2 requirements. The meaning of (C2[1](B2[3:7,2,1](A2[10]))) is that the second investigation section consists of 3 security objectives. The first security objective is expressed in terms of 7 security requirements. The second security objective is expressed in terms of 2 security requirements. The third security objective is expressed as one security requirement. The rest of the structure may be interpreted in an analogous manner. Notice the importance of viewing the ISO 17799 as an expert system. This standard becomes alive. While the SISAP verifies the organization compliance with the standard, it also allows the organization to perform a sensitivity analysis to identify where enhancement is feasible for the achievement of the desired security posture.

That is, the nominal audit is characterized with a great deal of interactions between the auditors and staff members, especially those who are involved in information security. A very important part of the evidence collected in the nominal audit stage is elicited from staff

members. The study of the company's conformity with the best security practices brought by the ISO 17799 produces a set of claims related to the 10 security sections included in the standard.

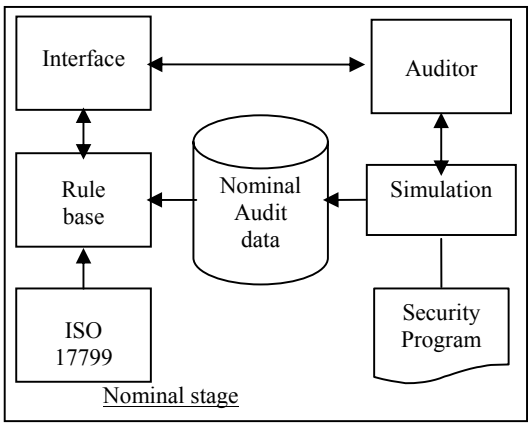

Figure 4: Simulation-based rule base generator of SISAP

Since the A structure constitutes the input layer of the rule base generator system, a dialog generation management system is needed to manage the interactions between information owners, users, and staff members from the organization side and the auditors. A semantic analysis is performed on the A concepts constituting the premises in the rule base generator system to parse the conditions sought by the auditors into more atomic concepts. Valid atomic concepts are those concepts that can be asserted or denied by posing a short sequence of simple questions. The SISAP develops a dialog generation management system made of hundreds of questions. The input layer acquires hence hundreds of input values elicited from information owners, staff members, and users using several data collection techniques, including interviews, show and tell, etc.

For example, The SISAP represents Section 3 of the ISO 17799 as the rule base chunk (C1[1](B1[1:2](A1[2]))) for which we develop the dialog generation subset provided in Figure 5. The target of the audit shows conformity with the concepts implicitly defined in the questions posed. The A concept contains the fusion of the evidence collected throughout the dialog defined for the rule base structure laid down for the corresponding section of ISO 17799.

(C1[1](B1[1:2](A1[2])))

A1.1's antecedents:

- The TOTA has a policy document that is approved by management, published and communicated, as appropriate, to all employees.
- The TOTA's policy document states management's commitment and sets out the organization's approach to managing information security.
- The TOTA's policy document contains a definition of information security, its overall objectives and scope and the importance of security as an enabling mechanism for information sharing.
- The TOTA's policy document contains a statement of management intent, supporting the goals and principles of information security.
- The TOTA's policy document contains a brief explanation of the security policies, principles, standards and compliance requirements of particular importance to the organization.
- The TOTA's policy is in compliance with legislative and contractual requirements.
- The TOTA's policy contains security education requirements.
- The TOTA's policy contains prevention and detection of viruses and other malicious software requirements.
- The TOTA's policy contains business continuity management requirements.
- The TOTA's policy contains consequences of security policy violations.
- The TOTA's policy contains a definition of general and specific responsibilities for information security management, including reporting security incidents.
- The TOTA's policy contains references to documentation, which may support the policy, e.g. more detailed security policies and procedures for specific information systems or security rules users should comply with.
- The TOTA's policy is communicated throughout the organization to users in a form that is relevant, accessible and understandable to the intended reader.

A1.2's antecedents:

- The TOTA's policy has an owner who is responsible for its maintenance and review according to a defined review process.
- The TOTA's policy has a process that ensures that a review takes place in response to any changes affecting the basis of the original risk assessment, e.g. significant security incidents, new vulnerabilities or changes to the organizational or technical infrastructure.
- The TOTA's policy has scheduled, periodic reviews of the policy's effectiveness, demonstrated by the nature, number and impact of recorded security incidents.
- The TOTA's policy has scheduled, periodic reviews of the policy's cost and impact of controls on business efficiency.
- The TOTA's policy has scheduled, periodic reviews of the policy's effects of changes to technology.

Figure 5: Dialog generation scheme for ISO 17799 [section 3]

4. Summarized SISAP Worksheets

The SISAP employs 39 elicitation worksheets, as in Standard Analytic Security Audit (SASA) developed for professional use:

- SISAP:NAW1:ABCSPW: Security Policy
- SISAP:NAW2:ABCOW: Organizational Security
- SISAP:NAW3:ABCCCW: Asset Classification And Control
- SISAP:NAW4:ABCPHW: Personnel security
- SISAP:NAW5:ABCPEW: Physical and Environmental Security
- SISAP:NAW6:ABCCOW: Communications & Operations Management
- SISAP:NAW7:ABCACW:Access Control
- SISAP:NAW8:ABCSDW: System Development and Maintenance
- SISAP:NAW9:ABCBCW: Business Continuity Management
- SISAP:NAW10:ABCCW: Compliance
- SISAP:NAW11:CLS1W:Security Policy
- SISAP:NAW12:CLS2W: Organizational Security Claims
- SISAP:NAW13:CLS3W: Asset Classification and Control Claims
- SISAP:NAW14:CLS4W: Personnel Security Claims
- SISAP:NAW15:CLS5W: Physical and environmental security Claims
- SISAP:NAW16:CLS6W: Communications and operations management Claims
- SISAP:NAW17:CLS7W: Access control Claims
- SISAP:NAW18:CLS8W: System development and maintenance Claims
- SISAP:NAW19:CLS9W: Business continuity management Claims
- SISAP:NAW20:CLS10W: Compliance
- SISAP:NAW21:CSPW: Corporate security posture worksheet
- SISAP:TAW1:APW: Asset Profile Worksheet
- SISAP:TAW2:VPW: Vulnerability Profile Worksheet
- SISAP:TAW3:TPW: Threat Profile Worksheet
- SISAP:TAW4:APVW: Asset P Vulnerability Worksheet
- SISAP:TAW5:ASVW: Asset S Vulnerability Worksheet
- SISAP:TAW6:ATVW: Asset T Vulnerability Worksheet
- SISAP:TAW7:TPVW: Threat P Vulnerability Worksheet
- SISAP:TAW8:TSVW: Threat S Vulnerability Worksheet
- SISAP:TAW9:TTVW: Threat T Vulnerability Worksheet
- SISAP:TAW10:AVTW: Asset Vulnerability by Threat Worksheet
- SISAP:TAW11:TVW: Threat Vulnerability Worksheet
- SISAP:TAW12:BRATW: B Risks of Assets by Threats Worksheet
- SISAP:TAW13:SCW: S Controls
- SISAP:TAW14:SAW: Security Analysis Worksheet
- SISAP:TAW15:AVTW: Secured Asset Vulnerability by Threat Worksheet

- SISAP:TAW16:RRATW:
  R Risks of Assets by Threats Worksheet
- SISAP:TAW17:SOA:
  Statement of Applicability Worksheet
- SISAP:AMW1:WFSW:
  Worksheet fillers Worksheet

The C concept corresponds to the fusion of the security objectives defined in the ISO 17799 to produce the corporate security posture. Confidence factors that are produced, at the nominal audit, are associated with the 10 security objectives imposed by the ISO 17799: 1) Security policy, 2) Organizational security, 3) Asset classification, 4) Personnel security, 5) Physical are produced, and environmental security, 6) Communications and operations management, 7) Access control, 8) Systems development and maintenance, 9) Compliance, and 10) Business continuity planning.

The nominal claims, in worksheets, SISAP:NAW11:CLS1W through SISAP:NAW 20:CLS10W show the auditors' preliminary evaluations of the company's security posture in terms of ISO 17799's requirements that are partially based on staff members' assessments. The nominal claims set the directions for the technical audit, and produces information that will be used in preparing the security testing activities needed to revise the current appraisal of the company's security posture. The nominal evidence is also useful to reconfigure the audit trail data stream employed in the technical audit stage.

The audit trail is used to guide the technical audit. To achieve better efficiency, only those variables that are relevant to the nominal claims are recorded in the audit trail.

5. Technical audit

The technical audit phase includes a revisit of the security policy to track any revisions or additions and review of the approved testing proscriptions produced from nominal claims. This leads to a precise definition of the scope of the technical audit. A random selection of information assets involved in the nominal claims will be subject of security testing activities engaged in vulnerability assessment and risk analysis. The size of the random sample of information assets included in testing activities may be statistically computed [10].

That is, the technical audit, as in BS 7799.2 consists of:

1-Security policy
2-Audit scope
3-PDCA-based RIAMS
4-Risk-driven security program

This article intentionally leaves out the details concerning testing activities prescribed in auditors claims produced at the nominal audit. Before further proceeding to the next section, it is very important to be familiar with the ISMS requirements imposed by BS 7799.2. It is also important to be familiar with the PDCA (Plan, Do, Check, and Act) cycle used as a framework in the risk identification, assessment, management, and security (RIAMS) approach presented below. Great attention is given in the literature to testing activities and available tools ([2], [5], [7], [8]). The technical audit phase is illustrated in Figure 6.

6. RIAMS framework

The RIAMS framework consists of four steps

1-Analysis of business value generation capabilities of assets
2-Analysis of asset vulnerabilities
3-Threat analysis
4-Security analysis

Most testing techniques involved in the technical audit are predominantly manually initiated and conducted. Members of the technical audit team should have significant security and networking knowledge, including significant expertise in one or more of the following areas: network security: firewalls, intrusion detection and response systems, operating systems, programming and networking protocols [5]. Following are some of the testing activities that may be ordered ([3], [4], [11]):

- Password Cracking
- Log Analysis
- Integrity Checkers
- Virus Detection
- War Dialing
- Network Mapping

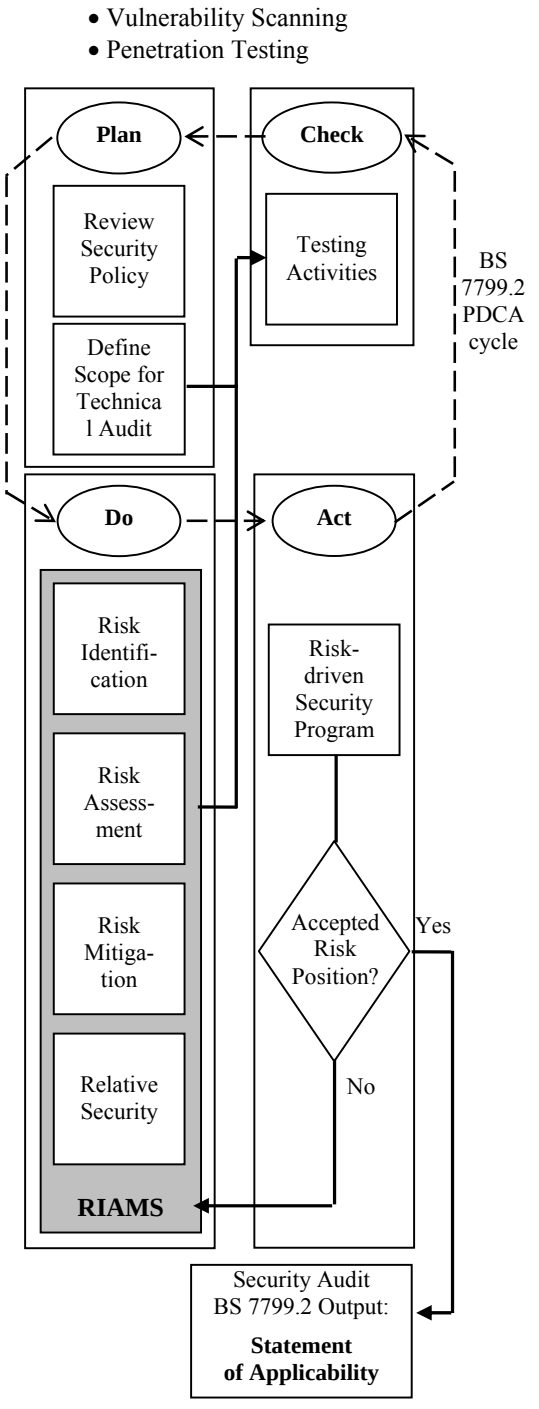

Figure 6: The SISAP technical audit phase is compliant with BS 7799.2

Often, several of these testing techniques are used in conjunction to gain more comprehensive assessment of the overall network security posture. For example penetration testing almost always includes network mapping and vulnerability scanning.

7. Analysis of business value generation capabilities of assets

This step defines the asset business value in dollars. It expresses the business value generation capability of the information asset. For example, if a print server is acquired at a total cost of $10,000 and has an annual business value generation capability of $120,000, is lost due to a joint threat-vulnerability condition, then the total loss is $120,000 and not $10,000. The annual business value generated by the information asset is equal to the total annual revenues generated by the asset minus the total annual costs of acquiring and operating the asset.

8. Analysis of vulnerabilities

This step defines the vulnerabilities on the asset. Of course, those vulnerabilities for which the threats do not exist do not represent an immediate danger, and no risk should be added to the corporate risk position. Each vulnerability should be related to a set of threats that can potentially transform this vulnerability into harm. There are many vulnerability assessment tools available in the literature and the market, for example, NESSUS, VLAD, Nikto, MBSA, SARA, TARA, etc. [6].

9. Analysis of relative security

This step defines the security controls to be implemented which will improve the company's risk position. Residual risk will be computed following the implementation of these security controls.

The security layer is the set of security controls implemented to improve the corporate risk position. Security controls are implemented to eliminate or reduce target vulnerabilities on information assets. A security control's effect on the vulnerabilities on assets should be evaluated along with its effects on the current corporate risk position before it is implemented. The security layer, for example, connects a set of threats to a set of vulnerabilities, and reduces the strengths of vulnerabilities to weaken the effects of the threats on information assets which will diminish their capabilities of business value generation.

10. Analysis of threats

This step defines the threats. Each threat is related to a subset of vulnerabilities identified on the assets. Risks are computed in terms of the effects of the threats on the assets given the current vulnerabilities. If vulnerability exists but the threat that can exploit it does not exist, or if the threat is present but the vulnerabilities to exploit do not exist, then there be no risk for the information asset in question.

11. The PDCA cycle in RIAMS

The PDCA cycle is a requirement in BS 7799.2. The SISAP incorporates the PDCA in its RIAMS steps as shown in the algorithm provided in Figure 7.

```
α0=Tolerated risk
R=Residual risks
B=Basic risks

While R risk > α0,
        While budget >0,
                Define a security control
                Compute R risk;
Plan: Security program= Retained security
controls
Do: Statement of applicability; Post-audit review
Check: Identify risks; Compute B risks;
Act: Manage risks.
```

Figure 7: PDCA-based RIAMS algorithm

12. Conclusion

This article presented some aspects of the SISAP security audit methodology. It showed that it is fully compliant with the ISO 17799 and BS 7799.2. The SISAP employed a simulation-based rule base generator that balances risks and business value generation capabilities using the PACD cycle imposed in BS 7799.2. The SISAP employed a concept proof approach based on 10 security investigation areas, 36 security objectives, and 127 security requirements. The auditor is given a variety of technical approaches for collecting, analyzing, and fusing audit evidence obtained at various steps of the security audit.

References

[1] Carlson, T, (2005), "Understanding ISO 17799", HotSkills, Inc., http://www.hotskills-inc.com.

[2] Herzog, P., (2001), "Open-Source Security Testing Methodology Manual", Available on http://www.ideahamster.org.

[3] Kapp, J., (2000) "*How To Conduct a Security Audit, PC Network Advisor"*, Vol.120, pp3-8, Available on http://www.itp-journals.com.

[4] Konigsberg, B., (2002), "Auditing Inside the Enterprise via Port Scanning & Related Tools", SANS Institute, Available on http://www.pcsupportadvisor.com/nasample/t04123.pdf.

[5] MIS-CDS, (2000), "An overview of network security analysis and penetration testing: A guide to computer hacking and preventions", Available on http://www.mis-cds.com.

[6] NISCC, (2000), "Introduction to vulnerability Assessment Tools", National Infrastructure Security Co-Ordination Centre, London.

[7] NIST, (2002) Guideline on Network Security Testing, *Special Publication 800-42*, Available on www.nist.gov.

[8] Page, P. (2003), *Security Audit: A continuous Process*, Version 1.4b, SANS Institute; Available on http://www.sans.org/.

[9] Raggad, B. (2000), "Corporate Vital Defense Strategy", Proceedings of the 23rd National IS Security Conference, NSA/NIST, Baltimore, MD.

[10] Raggad, B. (2005), "The simple information security audit process: SISAP", Electronic Proceedings of AoM/IAoM, Norfolk, VA.

[11] Zeltser, L. (2001), *Auditing UNIX Systems: A Case Study*, SANS Institute.

Dr. Bel G. Raggad is a Professor of Information Systems in the Seidenberg School of Computer Science and Information Systems, at Pace University, New York. Dr. Raggad obtained his Ph.D. from Pennsylvania State University, University Park, PA, in 1989. Dr. Raggad's research interest is Information Security and Intelligent Decision Support (Possibilistic Computing, Dempster-and-Shafer theory, Fuzzy Set theory, Genetic Computing, and Neural Computing). Dr. Raggad has written several monographs in the Information Security area, and has published articles in refereed journals, and proceedings, including the Journal of Computer Information Systems, Managerial Decision, Journal of Management and Information Processing, Journal of Industrial Management and Data Systems, etc.

Emilio Collar, Jr. received the B.B.A. and M.S. degrees in Information Systems from Pace University in 1993 and 1998 respectively, and the Ph.D. in Information Systems from the University of Colorado at Boulder in 2005. His research interests include programming code readability and information security. He has worked at IBM's Worldwide Olympic Technology Team and conducted research on their technology solution for the 1998 Nagano Olympic Winter Games and the 2000 Sydney Olympic Summer Games. He is currently an Assistant Professor of Management Information Systems at Western Connecticut State University.