

**An Analysis of How ISO 17799 and SSE-CMM Relate to the S-vector Methodology**  
**August 2004**

**Janine Spears, Russell Barton, William Hery**



**The Penn State eBusiness Research Center**

**401 Business Administration Building  
University Park, PA 16802**

**Phone: 814.863.7575 Fax: 814.865.9119  
Web: <http://www.ebrc.psu.edu>**

**PENNSSTATE**

---

SMEAL College of Business Administration

Corporate Sponsors: IBM • UNISYS • XEROX • AT&T Wireless • Delphi Ventures • SAP AG • CIGNA • TYCO • HP

# Contents

Contents .....	ii
Abstract .....	1
Author Biographies .....	2
1. Introduction .....	3
2. ISO 17799 Described .....	4
2.1 History of ISO 17799 .....	4
2.2 What ISO 17799 is and is not .....	4
2.3 Becoming BS7799 Certified .....	5
2.4 How ISO 17799 concepts can be applied to the S-vector methodology .....	5
Applicable ISO 17799 Areas .....	5
Potential Scoring Metric for Incorporated ISO 17799 Controls .....	6
3. SSE-CMM Described .....	7
3.1 History of SSE-CMM .....	7
3.2 What SSE-CMM is and is not .....	8
3.3 How SSE-CMM is organized .....	8
SSE-CMM Model .....	8
SSE-CMM Appraisal Method .....	10
3.4 How SSE-CMM concepts can be applied to the S-vector methodology .....	11
Applicable Process Areas .....	11
Applicability of the Capability Levels .....	12
4. How ISO 17799 and SSE-CMM may be collectively utilized by S-vector .....	13
5. How the S-vector methodology differs from ISO 17799 and SSE-CMM .....	13
6. Discussion .....	14
7. Future Research .....	14
Appendices .....	16
A - Suggested ISO 17799 controls for S-vector .....	16
Procedural Components .....	16
Structural Components .....	24
B - Areas of ISO 17799 not suggested as S-vector components .....	25
C – Description of SSE-CMM Process Areas .....	26
D – System Security Assessment Method (SSAM) Evaluation Template .....	32
References .....	33

## **Abstract**

This paper analyzes two security standards, ISO 17799 and SSE-CMM, to determine if and how each of these standards may be integrated into a web application security assessment tool called S-vector. Analysis suggests that security controls outlined in ISO 17799 can be incorporated into S-vector as procedural components. ISO 17799 controls may be mapped to specific data, specific web applications, or across multiple systems. Eleven of SSE-CMM's security-related process areas can be implemented into an S-vector implementation by providing a framework in which to administer procedural components. The capability levels of SSE-CMM measure a process' maturity and can be integrated into S-vector if scoring objectives are to measure process maturity and not the quality of process output. The SSE-CMM Appraisal Method (SSAM) provides a detailed appraisal plan. SSAM can provide value in an S-vector implementation if: a) capability levels are used as the metrics scheme, and b) it is acceptable to assess an SSE-CMM process area in its entirety as opposed to assessing base practices individually. Future research is required to define the scope of a supporting security infrastructure that is needed to ensure an effective S-vector implementation.

## Author Biographies

**Russell Barton** is Associate Dean for Research and Ph.D./M.S. Programs and Professor of Supply Chain and Information Systems in the Mary Jean and Frank P. Smeal College of Business at Penn State. He received a B.S. in Electrical Engineering from Princeton University and M.S. and Ph.D. degrees in Operations Research from Cornell University. After ten years in industry, most of that time at RCA's David Sarnoff Research Center, he returned to academia, teaching at Cornell from 1987-1990 and then joining Penn State. At Penn State, he has received more than \$1.5 million for research in statistical process control, the design of experiments, and computer simulation, and has worked with industry sponsors including Boeing, Fluke, Ford, General Motors, Hewlett-Packard, Intel, Lucent, New-Holland and Xerox. Dr. Barton has taught short courses in concurrent engineering, design for manufacturing, and the graphical design and analysis of experiments. He has recently completed a text, Graphical Methods for the Design of Experiments, published by Springer-Verlag. He has worked to increase the practice component of engineering education at Penn State, and has received one national, one university, three college and two departmental teaching and curriculum development awards since 1990. He is a senior member of IEEE and IIE, and a member of ASQ and INFORMS. He has held a number of service positions in the INFORMS Simulation Society and is currently president. He is Program Chair for the 2007 Winter Simulation Conference.

**William Hery** is an eBRC Research Center Fellow in the Mary Jean and Frank P. Smeal College of Business at Penn State. Dr. Hery has more than 25 years of experience in research and development in industrial R&D environments, and 8 years of university level teaching of mathematics and computer science. The focus of his research has been the application of computer science, operations research, and mathematics to the understanding of large systems in a variety of contexts. During the most recent eight years he has focused on information and communications security in distributed processing environments. He is currently helping to define and build the Cybersecurity component for the Polytechnic University's Urban Security Initiative. He is also an advisor to a government agency on a homeland defense project. In 2001, Dr. Hery retired from Lucent Technologies Bell Labs, where he was a Distinguished Member of Technical Staff in the Government Communications Lab. During most of his 18 years at Bell Labs, he led R&D projects related to the Defense and Intelligence communities, focusing the technologies of Bell Labs' forward looking research on the special needs of the government.

**Janine Spears** is a doctoral candidate in the department of Supply Chain and Information Systems in the Mary Jean and Frank P. Smeal College of Business at Penn State. She received a B.S. in Computer Information Systems from California State University at Los Angeles and an M.B.A. from Case Western Reserve University. Her research interest is in the management of information security. Prior to joining Penn State, Janine worked as a Business Systems Analyst at Twentieth Century Fox, Sony Pictures Entertainment, AST Computers, and the Jet Propulsion Laboratory. She also taught courses in information systems at Cuyahoga Community College, Santa Monica College, and California State University at Los Angeles.

# 1. Introduction

The purpose of this paper is to analyze ISO 17799 and SSE-CMM to determine if and how each of these two security standards may be integrated into the S-vector methodology. This is a scoring methodology, currently under development, for assessing web application security. S-vector development is a joint research project between Penn State University and Polytechnic University in collaboration with the Commonwealth of Pennsylvania's Office of Administration/Office for Information Technology (OA/OIT) (Barton et al, 2004).

The focus of the S-vector methodology is on the assessment of web applications. In general, the methodology functions as follows (Barton et al, 2004): The security requirements for each web application are mapped into a requirements vector that contains a target score. A periodic assessment of the web application yields a corresponding application score vector, which can be compared to the application's requirements vector. The goal of the S-vector methodology is to enable government agencies to prioritize security enhancement projects, evaluate security enhancement strategies, and to measure progress in improving web application security (Barton et al, 2004).

Three types of security requirements are mapped into S-vector: technical, structural, and procedural. Technical components include the security services an application provides, such as encryption and authentication (Hery & Liu, 2003). Structural components include the "software structures and designs that help assure the services will be delivered with greater assurance" (Hery & Liu, 2003). Examples include various types of automated programming code checks. Procedural components include the "development, deployment, and management procedures that help assure the services will be delivered with greater assurance" (Hery & Liu, 2003). Examples include software development methodology and system management policies.

Technical components, such as encryption and authentication, will largely correspond to the Common Criteria's Protection Profiles (Barton et al, 2004). This paper analyzes the applicability of ISO 17799 and SSE-CMM for structural or procedural requirements, and makes recommendations on specific aspects of each standard that can be incorporated into S-vector. The recommendations in this paper are intended for further discussion among the S-vector project team.

In addition to determining security elements for populating the vectors, current S-vector research is also evaluating metric schemes to quantify required and actual security results. Although analyzing and selecting a metric scheme is not the primary focus of this paper, a suggestion is provided on how S-vector elements related to ISO 17799 may be scored. Secondly, as part of the SSE-CMM analysis, its metric scheme of capability levels is described.

This paper is organized as follows: First, a detailed description of ISO 17799 is provided that contains the standard's history, usage, certification, and applicability to S-vector. Second, a detailed description of SSE-CMM is provided that contains the standard's history, usage, organization, assessment, and applicability to S-vector. Third, suggestions on how the two standards may collectively be integrated into the S-vector methodology are discussed. Fourth, differences between ISO 17799, SSE-CMM and the S-vector methodology are highlighted. Fifth, a discussion on overall findings and impressions is provided, followed by suggestions for future research. Finally, an appendix section contains detailed tables that list specific ISO 17799 controls and SSE-CMM process areas for recommendation, along with explanatory notes.

## 2. ISO 17799 Described

This section first provides a history of the ISO 17799 standard, and then clarifies what is and is not provided by the standard. Next, an explanation is given on how organizations become certified against BS7799. Finally, recommendations for applying ISO 17799 to S-vector are provided, along with an example of a potential implementation.

### 2.1 History of ISO 17799

ISO 17799, Information Technology – Code of Practice for Information Security Management, is an international standard that provides guidelines and controls for managing information security. Its origins are from a standard developed by Great Britain's Department of Trade and Industry (DTI) in 1993 for commercial use. The British Standards Institute (BSI) took ownership of the standard, and after making some revisions, renamed it to BS7799 in 1995. In the late 1990's there was increased demand for an international information security policy. However, BS7799 was not considered general enough. So BS7799 was revised in 1998 and again in 1999 before being adopted by the International Standards Organization (ISO) and fast-tracked to standardization to become ISO 17799 in December 2000. BS7799 Part 1 and ISO 17799 are essentially identical (ISO 17799 News – Issue 1), and are used as suggestions for choosing information security controls.

In 1999, BS7799 Part 2 was created as a standard for implementing information security controls. It is with BS7799 Part 2 that organizations become certified. ISO 17799 does not currently offer certification. However, it is expected that BS7799 Part 2 will become an ISO standard (ISO 17799 News – Issue 10), though no expected date is given.

### 2.2 What ISO 17799 is and is not

Information security is defined as the preservation of confidentiality, integrity, and availability. It is achieved by implementing controls, which may be policies, practices, procedures, organizational structures, or software functions. (ISO 17799)

ISO 17799 offers guidelines for safeguarding information assets by providing a list of information security controls. The standard contains 127 controls from 10 areas, which are listed later in this paper. Controls can be designated as organization-level or application-level controls. Organization-level controls apply to the security perimeter in which an organization operates and are needed for effective web application security. Application-level controls apply to individual web applications.

ISO 17799 suggests *what* security controls to include in a security program, but does not specify *how* to develop or administer them. It is not a technical standard, nor is it driven by specific technology. It does not provide a scoring mechanism or other methods for evaluation. However, it is said to be compatible with the Equipment Assurance Level (EAL) scoring of the Common Criteria, ISO 15408 (Bisson, St. Germain; Carlson, 2001).

ISO 17799 recommends that the selection of controls an organization employs be determined by: a) a risk assessment, b) legal, statutory, regulatory, and contractual requirements, and c) an organization's particular set of principles, objectives, and requirements for information processing. Although the

standard places a very strong emphasis on the need for a risk assessment, it does not provide guidelines for conducting a risk assessment. However, COBRA is a software tool (unofficially) associated with ISO 17799 and is used to facilitate conducting risk assessments (C&A Security Risk Analysis Group, 2003). ISO 17799 also does not provide security guidelines for specific legislation. Instead, it provides guidelines on safeguarding organizational records, which may be required as evidence in legal proceedings.

In addition to a risk assessment, ISO 17799 also places a strong emphasis on an organization defining a clear security policy. Details on how to develop such a policy is outside the scope of ISO 17799. However, general guidelines are provided on what a Security Policy Document should contain, and how it should be reviewed and evaluated.

### **2.3 Becoming BS7799 Certified**

Organizations seeking certification typically develop a, or modify their existing, security policy to match the controls outlined in ISO 17799. These organizations typically purchase a toolkit containing both standards ISO 17799 and BS 7799 Part 2, along with a set of predefined security policies that correspond with the controls outlined in ISO 17799. A security team is established, policies are implemented, and eventually a certifying body evaluates the organization's compliance. If the organization is in compliance, it becomes certified.

Each country has representatives assigned to the ISO standards committee. The representatives appoint an accreditation body that can audit and certify organizations against BS7799 Part 2. The US does not have an accreditation body. Therefore, US organizations seeking ISO 17799 certification must become certified by a country that does have accreditation. Alternatively, US organizations can seek consultation from a non-accredited ISO 17799 consultant and become ISO 17799 compliant without becoming officially certified.

As of March 2003, only three U.S. firms had become certified (Small & Brykczynski, 2003), while internationally, over 80,000 firms are said to be ISO 17799 compliant (Callio Technologies). Those US firms that use ISO 17799 appear to use it as a guideline and select specific controls applicable to their environment. In other words, they do not seek certification of the entire standard. Instead, firms seek compliance with portions of the standard relevant to their operations.

### **2.4 How ISO 17799 concepts can be applied to the S-vector methodology**

This section provides a list of recommended ISO 17799 areas to be incorporated into an S-vector implementation. ISO 17799 does not contain a scoring metric for evaluating implemented ISO 17799 controls. The second part of this section describes a potential scoring metric that could be applied to an S-vector implementation containing ISO 17799 controls.

#### Applicable ISO 17799 Areas

As discussed in the Introduction, the S-vector has technical, structural, and procedural components. ISO 17799 "controls" primarily relate to S-vector's procedural components. Table 1 below indicates which of the ten ISO 17799 areas are recommended for S-vector, as well as which areas currently map to S-vector components as outlined in Strawman S-vector Structure (Hery & Liu, 2003). Recommended ISO 17799 controls include both application-level and organization-level controls that impact web application

security. Recommended ISO 17799 controls that do not map to S-vector components outlined in the Strawman generally relate to organization-level controls that apply across applications. While the S-vector methodology implicitly relies on organizational policies that classify assets and determine security requirements, components outlined in the Strawman are generally at the application level since the focus of S-vector is on web application security. However, recommended organization-level ISO 17799 controls can be incorporated into S-vector to ensure those policies required for an effective S-vector implementation are developed and executed. For details on security controls within each ISO 17799 area, please refer to Appendices A and B.

ISO 17799 areas	Recommended for S-vector	Maps to S-vector Components		
		Procedural	Structural	Technical
Security policy	X	X		
Organizational security	X			
Asset classification and control	X			
Personnel security	X			
Physical and environmental security				
Communications and operations management				
Access control	X		X	
Systems development and maintenance	X	X	X	
Business continuity management				
Compliance				

Table 1. ISO 17799 areas related to S-vector

S-vector will not be used to define suggested policies and controls from ISO 17799. Instead, S-vector can be used to evaluate the existence, quality, or maturity of relevant security policies and controls. The remainder of this section suggests how ISO 17799 controls may be implemented as S-vector’s procedural components.

#### Potential Scoring Metric for Incorporated ISO 17799 Controls

A requirements vector is established containing a list of relevant ISO 17799 controls. OA/OIT management effectively checks which controls they will implement. A 5-level scale, analogous to the 5-level scale used in academia (A, B, C, D, F), can be used for scoring the quality of each control. For the requirements vector, each checked control receives a target score of 1-5, indicating the desired quality of the control. Desired quality level is commensurate with the priority level attributed to the control. Unchecked controls receive a value of “0”.

During a security appraisal, the existence and quality of each checked control is evaluated. A score, analogous to an academic grade, is assigned to each control. Scores populate a scoring vector of actual security results. The scoring (or actual) vector contains the same elements as the requirements vector. The highest score that can be achieved per element (i.e., control) in the scoring vector is the associated target score. Actual scores are then compared to target scores.

Vector elements, representing procedural controls, may be grouped and sub-grouped by scope and topic. For example, all procedural controls (group) can be broken down by organization-level and application-level controls (sub-groups). Organization-level controls can then be further grouped by topic, such as Information Security Policy Document, Access Control Policy, etc. Another example is that application-level controls can be grouped per application. Scores can be sub-totaled by group and sub-group(s) in order to compare scores across groupings.

Since procedural controls are more subjective than technical controls, effective scoring depends on precise definitions and scoring criteria being developed for each procedural control. Scoring criteria may be outlined in a checklist. The reviewer can then evaluate the actual implementation against the checklist. In some cases, the scoring criteria may merely specify the “existence” of a control.

An example of the implementation described above is now provided. The ISO 17799 control “Separate system utilities from application software” (related to Operating System controls) may be assigned a target score of “3” for its desired quality level that is commensurate with its assigned priority. The scoring criteria may be that all system utilities are stored on a separate drive (or server) from application files. If all the system files are stored in a separate location from application files, a score of 3 is assigned (the highest score is the target score). If system files are stored on the same drive as application files, a score of 0 is assigned. Alternatively, the criteria may indicate degrees of quality. Using the same control as an example, a score of 3 is assigned if 100% of all system and application files are stored separately; a score of 2 is assigned if 75% or more, but not all, system and application files are stored separately; a score of 1 is assigned if 50%-74% of all files are stored separately. A score of 0 indicates the control has not been implemented. This control could be grouped in the following hierarchy by scope and topic: Procedural components → Organization-level controls → Operating System controls → Separate system utilities from application software. Scores may be sub-totaled for each of these groupings.

In summary, selected ISO 17799 controls can be used as procedural components within a security vector. The controls may apply across multiple systems (organization-level) or to individual web applications. A target score is assigned based on the relative importance of the control. During an appraisal, an actual score is determined based on pre-defined criteria. The actual score is compared to the target score. Cumulative scores may be computed per group and sub-group of controls as desired.

### **3. SSE-CMM Described**

This section first provides a history of the SSE-CMM standard, and then clarifies what is and is not provided by the standard. Next, an explanation is given of the components of SSE-CMM and how they are organized. Finally, recommendations for applying SSE-CMM to S-vector are provided.

#### **3.1 History of SSE-CMM**

The Systems Security Engineering Capability Maturity Model (SSE-CMM) project was initiated in 1993 as an NSA-sponsored effort to develop a CMM for security engineering. Over sixty organizations were involved in the effort. The SSE-CMM project resulted in a model and an appraisal method. The first version of SSE-CMM model was published in October 1996, and the appraisal method in 1997 (SSE-CMM, 2003). Pilot testing of the model and appraisal method was conducted in 1996 and 1997, which resulted in revised SSE-CMM version 1.1. Following the release of version 2, the International Systems Security Engineering Association (ISSEA) was formed in 1999 to continue the development and

promotion of SSE-CMM (SSE-CMM, 2003; ISSEA, 2004). SSE-CMM became an ISO (international Organization for Standardization) standard in 2001 as ISO/IEC 21827 (EOS, 2001). SSE-CMM Version 3, the latest version as of this writing, was developed in June 2003 and is the version referenced in this paper.

CMM is a registered trademark of Carnegie Mellon University. Several engineering CMMs have been developed. The CMMs most directly related to SSE-CMM are Software Engineering Institute CMM (SW-CMM) and the Systems Engineering CMM (SE-CMM). In 1991, SW-CMM became the first CMM developed for software development; subsequently, SE-CMM was developed (CMU, 2004). Of the twenty-two security engineering process areas in the SSE-CMM model, eleven are related to project and organizational processes and were adapted from, and nearly mirror, those from SE-CMM. Currently, both SW-CMM and SE-CMM, have been integrated into the Capability Maturity Model Integration (CMMI). CMMI's aim is to reduce redundancy by merging multiple CMMs into a single, integrated engineering approach (CMU, 2004).

### **3.2 What SSE-CMM is and is not**

SSE-CMM is a capability maturity model (CMM) for systems security engineering (SSE). A Capability Maturity Model (CMM) is a framework for developing a process – typically an engineering process – from an informal, adhoc process into a structured, institutionalized process. A process may be introduced within an organization through informal use on a single project. As the process matures, it will be formally defined, documented, institutionalized (implemented across the organization), and the organization will actively seek to continuously improve the process. The idea is that as a process matures, results from the process become more stable, and therefore predictable, controllable, and effective in terms of costs, productivity, and quality (SSE-CMM, 2003).

SSE-CMM is comprised of two parts: a) a model for security engineering processes and project and organizational processes, and b) an appraisal method for assessing the maturity of those processes. The process areas do not recommend specific methodologies, controls, or guidelines. The appraisal method employs SSE-CMM's capability levels, which are used to assess the maturity of a process, not the quality of its output.

SSE-CMM can be applied in 3 ways: a) process improvement, b) capability evaluation, and c) assurance. Process improvement is accomplished by achieving higher capability levels for a given process. A customer that ascertains the capability level of a vendor organization seeking to provide the customer with its products or services accomplishes capability evaluation. Assurance is achieved by providing evidence that a given process has reached maturity.

### **3.3 How SSE-CMM is organized**

#### SSE-CMM Model

The SSE-CMM model is organized in two parts: domain and capability levels. The domain contains a list of practices that embody security engineering. Domain-related practices, referred to as *base practices*, are grouped by topic, referred to as a *process area*. A capability level is assigned to each process area and is used to indicate the level of maturity a process has achieved. Capability levels are determined by successful completion of *generic practices*. A process area's base practices are evaluated against generic

practices to determine the capability level. Generic practices apply to all process areas and are grouped into *common features*. The model's structure is illustrated in Figure 1 below.

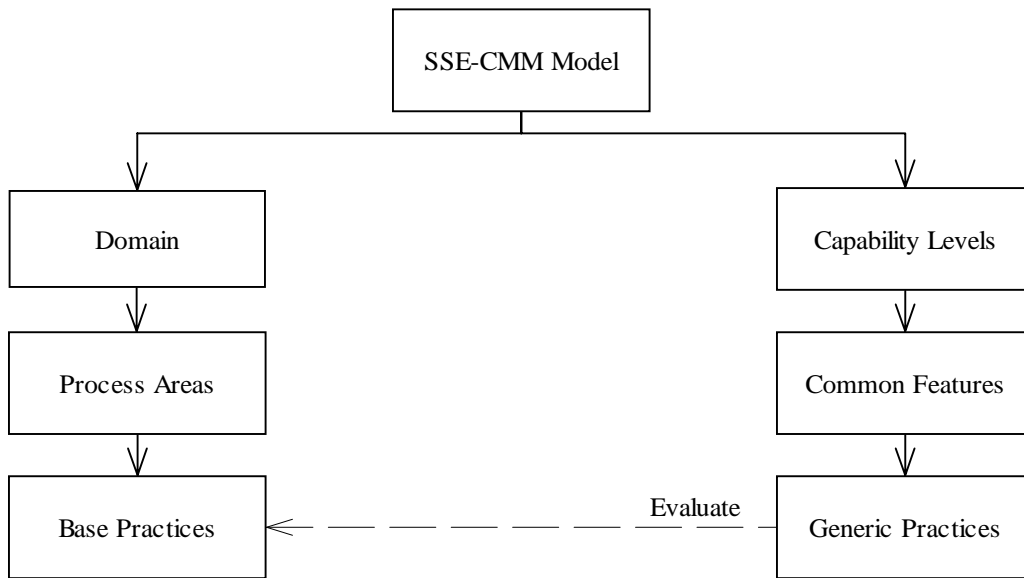


Figure 1. SSE-CMM Model Structure

SSE-CMM has twenty-two process areas (PA) and 129 base practices. The first eleven process areas (PA01 – PA11) are directly related to security engineering practices. The remaining eleven process areas (PA12 - PA22) were adapted from SE-CMM and focus on general organizational and project systems engineering practices. Each PA contains goals, a set of base practices, and examples of output from the PA. This paper only recommends, and therefore focuses on, the eleven security-related process areas.

SSE-CMM contains five capability levels used to indicate the level of process maturity. Capability levels are ordered from lowest to highest, with Level 1 being the lowest capability. Each capability level contains anywhere from one to four common features, as indicated in Figure 2 below. Common features represent a group of generic practices, or activities, that are performed to achieve a given capability level. Capability levels are achieved in sequential order. For example, Level 4 cannot be achieved until Levels 1 through 3 are achieved.

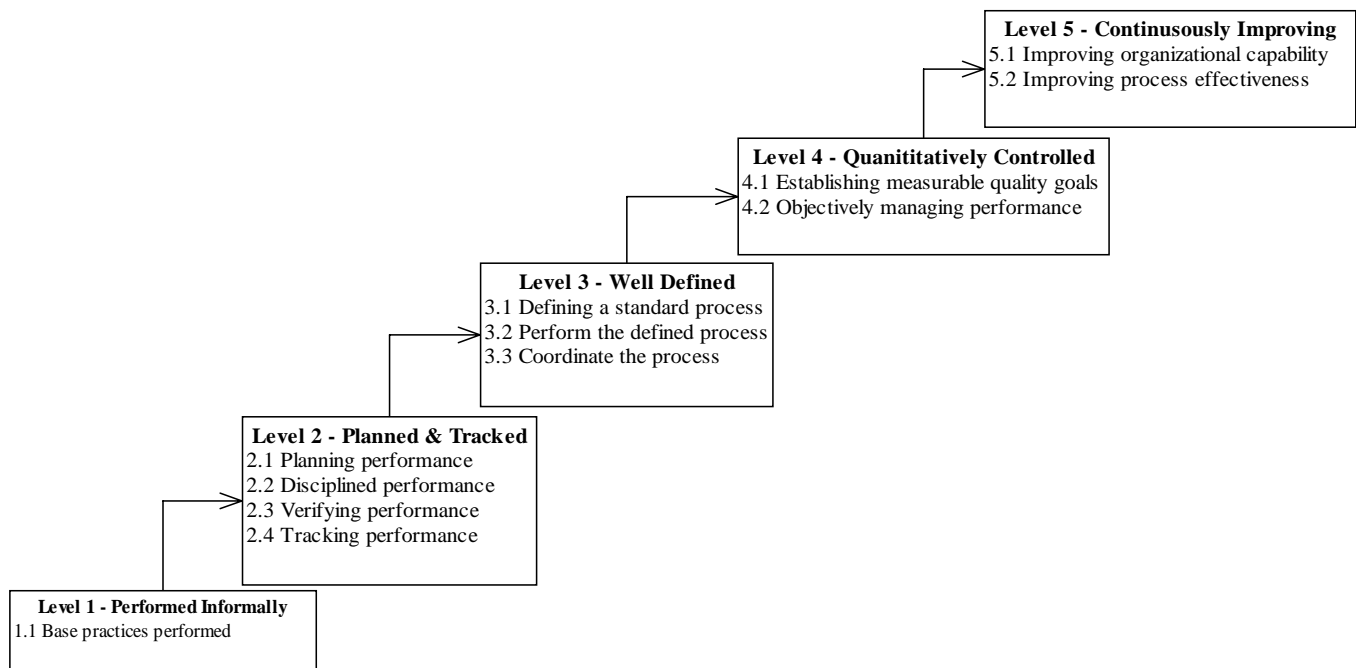


Figure 2. SSE-CMM Capability Levels

Level 1 indicates *all* base practices of a process area are being performed on an informal basis. Informal generally means undocumented, unstandardized, and possibly adhoc in nature. All base practices within a process area must be implemented in order for the process area to be considered implemented by an organization.

A process that has a Level 1 capability is generally only performed on a single project. As a process reaches higher levels of maturity, it becomes formally defined, monitored, tracked, and implemented throughout an organization. SSE-CMM defines an organization as an entity responsible for the oversight of multiple projects. Levels 1 and 2 relate to a specific project, while Levels 3 – 5 relate to organization-wide practices. The idea is that a process must be tried, tested, and understood at the project level before expanding its use organization-wide. Secondly, all common features within a capability level must be achieved before that capability level can be awarded.

### SSE-CMM Appraisal Method

The System Security Appraisal Method (SSAM) outlines how to plan, prepare, conduct, and report an SSE-CMM appraisal. The methodology uses a questionnaire to capture responses to, and evidence of, process maturity of the twenty-two process areas. A data-tracking sheet is used to tally scores from questionnaire responses in order to calculate a final percentage rating. The percentage ratings can then be compared across applications and systems.

The SSAM is a separate document developed by the SSE-CMM Project. In addition to a questionnaire template, the document contains detailed guidance on the following phases of an appraisal:

1. Planning (appraisal goals, scope, plan)
2. Preparation (questionnaire, system engineering documents to gather, interview questions)
3. On-site visit for conducting appraisal (includes a detailed agenda for a week-long appraisal)
4. Post-appraisal (wrap-up of analysis, report to present to appraisal sponsor)

### 3.4 How SSE-CMM concepts can be applied to the S-vector methodology

As explained in the previous section, SSE-CMM is comprised of process areas and capability levels – either or both of which can be applied to S-vector. In other words, it is possible to incorporate the eleven security-related process areas as procedural components within S-vector while using a metric scheme different from SSE-CMM’s capability levels. Likewise, it is possible to apply SSE-CMM’s capability levels as a metric scheme for assessing the maturity of all S-vector procedural components regardless if components originate from SSE-CMM’s process areas or not.

#### Applicable Process Areas

Each of the eleven security-related process areas is geared toward building a management framework in which to administer security controls across a project or organization. The remaining eleven process areas are general practices that apply to systems engineering in general, and are believed to be outside the scope of S-vector, so therefore are not recommended for an S-vector implementation. I believe that all eleven security-related process areas are applicable to an S-vector implementation. The Strawman S-vector Structure (Hery & Liu, 2003) is geared toward individual web applications, while SSE-CMM encompasses a larger scope that builds a security framework across applications. Consequently, although eleven SSE-CMM process areas may be applicable to an S-vector implementation, only two map to components listed in the Strawman, as indicated in Table 2 below.

SSE-CMM Security-Related Process Areas	Recommended for S-vector	Maps to S-vector Components		
		Procedural	Structural	Technical
PA01 Administer Security Controls	X	X		
PA02 Assess Impact	X			
PA03 Assess Security Risk	X			
PA04 Assess Threat	X			
PA05 Assess Vulnerability	X			
PA06 Build Assurance Argument	X			
PA07 Coordinate Security	X			
PA08 Monitor Security Posture	X	X		
PA09 Provide Security Input	X			
PA10 Specify Security Needs	X			
PA11 Verify and Validate Security	X	X		

Table 2. SSE-CMM process areas related to S-vector

For a list of each of these process areas’ corresponding base practices and explanatory comments, please refer to Appendix C. This appendix also lists PA12 – PA22, along with a brief explanation of how security-relevant portions of these PA’s may be handled via PA01 – PA11.

SSE-CMM lists the eleven security-related process areas in alphabetical order and does not provide, nor recommend, a sequential order of execution. However, Figure 3 below is provided in an effort to visualize how the various process areas are believed to inter-relate.

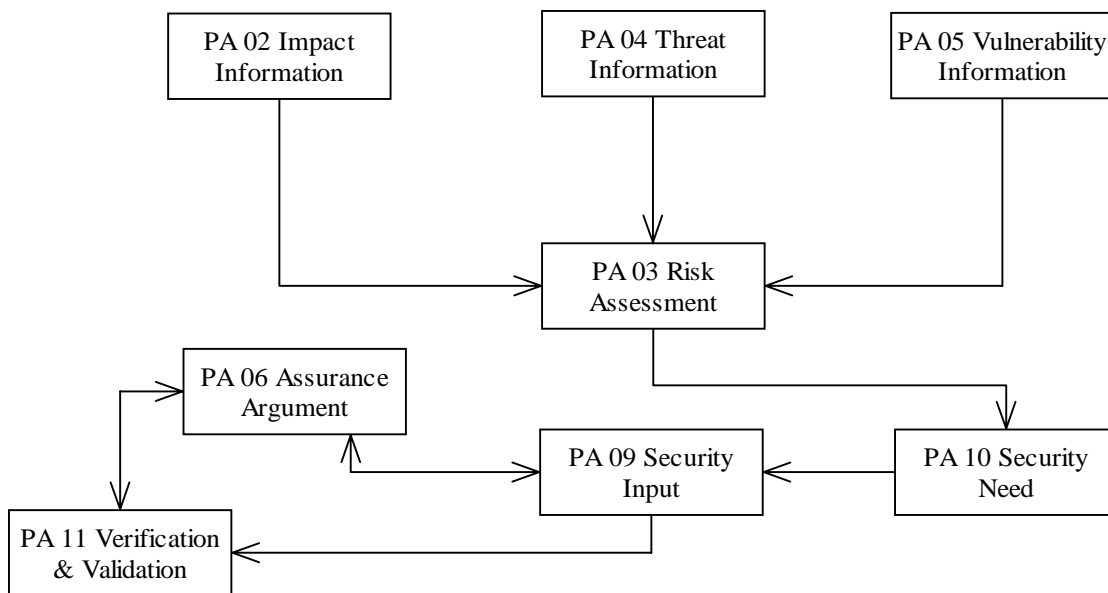


Figure 3. Relationships between SSE-CMM Security-related Process Areas

SSE-CMM process areas provide a management framework because they are at a high level of abstraction. Specific methodologies are neither recommended nor provided. The process areas aid in building a framework by outlining the need to identify, define, prioritize, and monitor security-related practices across a project or organization. The specific details on how to accomplish these practices are not provided. Once the base practices of a process area have been implemented, the maturity of those processes is assessed via the generic practices associated with capability levels.

### Applicability of the Capability Levels

The capability levels are used to assess the maturity of a given process. Their applicability depends on an S-vector component's scoring objective. If the objective is to assess the *quality* of a process' output, the capability levels may not be appropriate because they are not designed for this purpose. However, the capability levels are applicable to S-vector if a component's scoring objective is to determine that the component has been well defined and is being tracked and monitored.

A requirement S-vector can be populated with a target capability level. An assessment is then performed to determine the actual capability level. Capability levels can be assessed in strict conformance to SSE-CMM guidelines via the generic practices for each capability level. Or the assessment of the capability levels can be personalized to accommodate S-vector or OA/OIT scoring objectives.

If the capability levels are applied to S-vector, it would be helpful to use the SSAM for conducting appraisals because the appraisal methodology is provided in detail. It is, however, important to understand how SSAM assesses capability levels per process area. In general, SSAM assesses each base practice (BP) individually for capability level 1 to determine if each BP is performed – at least informally. For the remaining capability levels 2 – 5, the process area as a whole is assessed to determine the maturity of the entire process area. This means that SSAM does not assess the maturity level of individual BPs within a PA. As a result, it is possible for a PA to be awarded a high capability level, while there are BPs within that PA that are insufficiently implemented. Secondly, the SSAM assumes that an SSE-CMM appraisal is either performed in conjunction with an SE-CMM appraisal, or processes similar to those outlined in SE-CMM (or SSE-CMM PA12 – PA22) are in place prior to the appraisal.

#### **4. How ISO 17799 and SSE-CMM may be collectively utilized by S-vector**

The eleven security-related process areas in SSE-CMM can be used by OA/OIT to develop and administer a security framework. ISO 17799 can be used as a guideline for specific security controls (procedural and structural, not technical) that can in turn fit into the security framework established by SSE-CMM. SSE-CMM provides a higher level of management abstraction than does ISO 17799, which makes possible the use of both standards in support of an S-vector implementation. ISO 17799 provides specific controls that can populate security vectors for application security, while SSE-CMM establishes a mature, institutionalized framework for security administration. Both elements are critical success factors for an S-vector implementation. Specific controls are needed to populate security vectors (ISO 17799). However, a security infrastructure must be in place in order for these controls to be developed, monitored, measured, and controlled (SSE-CMM).

No overlap or redundancy is found between ISO 17799 and SSE-CMM. In fact, the two standards complement each other. For example, SSE-CMM has a process area for *administering* controls; however, recommended controls are not provided. ISO 17799 recommends controls, but does not provide details on how to administer those controls. Another example is that ISO 17799 recommends conducting periodical risk assessments. However, SSE-CMM takes this recommendation a step further by assessing the maturity of a risk assessment process. Finally, it is possible to apply SSE-CMM capability levels to ISO 17799 controls – provided the scoring objective is to assess the maturity of the control and not the quality of the output from the control.

The benefit of using SSE-CMM to develop and maintain a security framework is that by following the model, there is a higher assurance that the processes put in place will reach a desired level of maturity and will be maintained on a continuous basis. Otherwise, an asset inventory, a risk assessment, or a security policy document could be developed and not maintained. This would result in an outdated security framework and outdated policies, which would lead to ineffective system security.

The benefit of integrating ISO 17799 controls into S-vector procedural components is that ISO is an internationally recognized standard. ISO 17799 offers a comprehensive set of procedural controls that can be used to support web application security.

#### **5. How the S-vector methodology differs from ISO 17799 and SSE-CMM**

S-vector provides a mechanism for assessing a web application and comparing the actual score against a target score. While ISO 17799 provides a list of security controls as guidelines, it does not provide a method for evaluating the implementation of those controls. SSE-CMM provides a framework for administering security processes. However it does not provide the level of detail required of S-vector to assess web application security. For example, SSE-CMM does not contain processes for protecting data through encryption, authentication, etc.

The S-vector methodology contains technical, procedural, and structural components, and therefore provides a more comprehensive assessment of web application security than ISO 17799 and SSE-CMM. Neither of these two standards contains all three types of components. However, ISO 17799 and SSE-CMM provide elements that may be used to populate procedural components of an S-vector. They also provide guidelines for a security infrastructure that operates across applications.

## **6. Discussion**

The focus of the S-vector methodology is on the security of web applications. However, it is understood that a supporting security infrastructure is needed in order to develop an asset inventory, a risk assessment, and security policies that result in the requirements to be mapped into S-vector. SSE-CMM process areas are geared toward policies at the project or organizational level. Many of ISO 17799 controls are also geared across a project (e.g., operating system, networks, servers) or organization (e.g., security policy). S-vector is geared toward assessing the security of individual web applications and their data. Are the ISO 17799 controls and SSE-CMM process areas that are recommended in this paper as S-vector procedural components within S-vector's scope? If so, how can these activities be performed while meeting our objective of a low-cost assessment tool for web applications? If not, how can S-vector be effectively implemented without a defined administrative security framework that determines and incorporates security risks and requirements into S-vector?

Since both an asset inventory and risk assessment provide critical input into security requirements, an effective S-vector implementation requires these activities be performed at an effective level of detail. Consequently, the S-vector project team may want to recommend specific methodologies for accomplishing these activities. This is particularly significant if asset inventories and risk assessments are determined to be outside the scope of S-vector components, in which case they may not go through a formal appraisal process.

## **7. Future Research**

Further research is required to define the scope of the supporting security infrastructure that is needed to ensure an effective S-vector implementation. A supporting security infrastructure includes the development and on-going updates of an asset inventory, risk assessment, and security policies based on legal, regulatory, and organizational requirements. Defining the scope of the supporting security infrastructure that is required for an effective S-vector implementation will determine which of the recommendations in this paper can be incorporated as S-vector components.

Additional research is needed to locate academic research or industry feedback on implementing security standards such as ISO 17799 and SSE-CMM. In particular, limitations and challenges of implementing security standards (or aspects thereof) must be assessed.

The recommendations in this paper primarily address S-vector procedural components; further research is needed to determine structural components. In addition, an analysis of both security and automated testing software is needed to determine to what degree the validation of S-vector structural components related to web application code can be automated.

Future research is needed for selecting a scoring metrics scheme. Before a scoring metric can be selected, it is necessary to confirm a core set of S-vector technical, procedural and structural components. Once a core set of S-vector components is confirmed, researchers can confirm scoring objectives – either to assess the existence of a component, its quality, maturity, or a combination of these. Knowledge of scoring objectives would enable more effective analysis and comparison of alternative scoring metrics. Scoring objectives would also enable researchers to determine if one or multiple scoring metrics are

needed for an S-vector implementation. Scoring metrics to compare include, but are not limited to, the capability levels of the SSE-CMM and the Evaluated Assurance Levels (EAL) of the Common Criteria.

## Appendices

### A - Suggested ISO 17799 controls for S-vector

This section contains a table of ISO 17799 controls suggested for populating S-vector component vectors. With the exception of four structural controls, the majority of the suggested controls are procedural in nature. Recommended ISO 17799 controls relate to web application security, system security that impacts web applications (e.g., operating system, networks), and infrastructural security policies and controls that impact web application security. Controls are paraphrased from the standard. The controls listed are typically a summary of the relevant section and do not contain all of the controls and detail provided in the standard.

#### Procedural Components

ISO 17799 Section	Topic	Controls	Comments
3.1.1	Information Security Policy Document	<ol style="list-style-type: none"> <li>1. Objectives and scope of information security</li> <li>2. Policy for allocating security roles &amp; responsibilities within OA/OIT</li> <li>3. Policies for security education</li> <li>4. Policies for prevention &amp; detection of viruses &amp; other malicious software</li> <li>5. Policies for compliance with legislative &amp; contractual requirements</li> <li>6. Policies for business continuity management</li> <li>7. Policies for consequences of security policy violations</li> </ol>	
3.1.2	Information Security Policy Document Review & Evaluation	<ol style="list-style-type: none"> <li>1. Information Security Policy document has an assigned owner</li> <li>2. (Annual) review of policy effectiveness as determined by number, nature, &amp; impact of reported security incidents</li> <li>3. Update policy as needed by incorporating (annual) reassessment of current security risks</li> </ol>	
4.1.1	Management information security forum	<p>Management body that:</p> <ol style="list-style-type: none"> <li>1. Reviews and approves security policy and responsibilities</li> <li>2. Monitors significant changes to security threat exposure</li> <li>3. Reviews and monitors information security incidents</li> <li>4. Approves major information security initiatives</li> </ol>	Including this control in an S-vector implementation ensures the existence of a management forum for overseeing security initiatives.

ISO 17799 Section	Topic	Controls	Comments
4.1.2	Information security co-ordination	Coordinate roles, responsibilities, methodologies, and procedures across the organization	
4.1.3	Allocation of information security responsibilities	<ol style="list-style-type: none"> <li>1. Assets and security processes associated with each individual system are identified and clearly identified</li> <li>2. Manager is responsible for each asset or security process, and detailed responsibilities are document</li> </ol>	
4.2	Security of third-party access	<ol style="list-style-type: none"> <li>1. Policies on type and reasons for access by third parties</li> <li>2. Specification of information security requirements included in third-party contract (include general policy, controls, restrictions)</li> </ol>	ISO 17799 provides recommendations on particular security controls to cover in a third-party contract. Similar controls are generally accounted for in S-vector (e.g., access control, physical security, right to conduct audits, etc.); however controls in 4.2 and 4.3 ensure that such policies specifically address access by third-party contractors (i.e., outsourced IT operations).
4.3	Outsourcing	<p>When IT operations are outsourced, contract or policies specify how:</p> <ul style="list-style-type: none"> <li>▪ subcontractors are made aware of security responsibilities</li> <li>▪ integrity and confidentiality are maintained and tested</li> <li>▪ level of physical security for outsourced equipment</li> <li>▪ right to audit</li> </ul>	
5.1.1	Inventory of assets	Contains high-level guidelines for taking an inventory of assets, classifying their level of sensitivity, and assigning an owner. Section 5.2 contains guidelines for developing handling procedures for, such as copying, storage, electronic transmission, voice transmission, destruction.	ISO 17799 does not provide details on how to perform an asset inventory. An asset inventory serves as input into risk analysis, which in turn determines security requirements.
5.2.1	Classification guidelines	Scheme for classifying information assets to ensure the appropriate level of security protection	

ISO 17799 Section	Topic	Controls	Comments
6.1	Personnel security	<ol style="list-style-type: none"> <li>1. Identity check (e.g., passport, driver's license)</li> <li>2. Credential checks during application process (e.g., employment history, degrees)</li> <li>3. Character checks during application process of candidate employee (e.g., professional &amp; personal references)</li> <li>4. Signing of a confidentiality (non-disclosure) agreement</li> <li>5. Background security check (for handling highly sensitive data)</li> </ol>	<p>Although an identity check (and credential &amp; character checks) may be standard practice for internal employees, OA/OIT may want to consider requiring these checks for contractors, consultants, and any other external personnel that handle security assets.</p> <p>OA/OIT may also want to consider periodically reviewing the credentials for internal employees newly assigned to handle sensitive security assets.</p>
6.2	User security training	Train all employees on organizational security policies, procedures, and requirements; legal responsibilities; business controls; correct use of information processing facilities (e.g., logon procedures, software use, etc.)	
6.3	Responding to security incidents and malfunctions	<ol style="list-style-type: none"> <li>1. Communicate procedures to all personnel (&amp; external users) on how to report a security incident (e.g., security breach, threat, weakness, or malfunction)</li> <li>2. Train data owners, IT staff, and other designated personnel on response action to be taken upon receipt of an incident report</li> <li>3. Train data owners, IT staff, and other designated personnel on methodology for categorizing and quantifying (cost of incident and frequency of occurrence) security incidents</li> <li>4. Communicate disciplinary process for personnel that violate security policy</li> </ol>	ISO 17799 does not provide details for security incident reporting. However, the accomplishment of these criteria implies that procedures have been developed and communicated.
8.1.3	Incident management procedures	<ol style="list-style-type: none"> <li>1. Procedures established to cover all potential types of security incidents (e.g., denial of service, confidentiality breach, etc.)</li> <li>2. Audit trails for evidence and analysis</li> <li>3. Action plan for recovering from security breaches</li> </ol>	
9.1.1	Access Control Policy	<ol style="list-style-type: none"> <li>1. Identification of all information related to business (web) applications</li> <li>2. Policies for information dissemination &amp; authorization</li> <li>3. Development and usage of standard user access profiles</li> </ol>	

ISO 17799 Section	Topic	Controls	Comments
		<ul style="list-style-type: none"> <li>for common categories of jobs</li> <li>4. Usage of unique user IDs for accessing systems</li> <li>5. Policies for verifying user authorization prior to providing system access</li> <li>6. Policies for immediate removal of user access when user has changed jobs or left organization</li> <li>7. Generate and periodically review a formal report of all persons registered to use an application or service</li> </ul>	
9.2.2 9.53	Privilege management	<ul style="list-style-type: none"> <li>1. Identify privileges (any feature that enables a user to override system or application controls) for each system product (e.g., operating system, database, each application) along with the categories of staff to which the privileges can be allocated</li> <li>2. Policies for allocating, controlling and restricting privileges</li> </ul>	ISO 17799 indicates that inappropriate use of system privileges is often a major contributory factor in security breaches (section 9.2.2). Examples of privileges include manager, supervisor, or administrator system log-on access (i.e., group roles defined by an operating system).
9.31 9.54	Password use	<ul style="list-style-type: none"> <li>1. Develop and communicate user guidelines for choosing and safeguarding passwords</li> <li>2. Policy for changing passwords policy within specific time intervals</li> <li>3. Policy for advising users to change passwords whenever there is any indication of possibly system or password compromise</li> <li>4. Maintain a record of previous user passwords (e.g., for the previous 12 months) and prevent re-use</li> <li>5. store password files separately from application system data</li> <li>6. store passwords in encrypted form using a one-way algorithm</li> <li>7. Alter default vendor passwords following software installation</li> </ul>	
9.4.1	Policy on use of network services	Policy covering access and authorization of networks and network services	
9.4.2	Enforced path	Policy for limiting the routing options at each point the network through predefined choices	<p>Some examples provided in ISO17799 include:</p> <ul style="list-style-type: none"> <li>1. Enforcing use of security gateways for external network users</li> </ul>

ISO 17799 Section	Topic	Controls	Comments
			2. Restricting network access by setting up separate logical domains (e.g., VPNs) for user groups within the organization 3. Preventing unlimited network roaming 4. Limiting menu and submenu options for individual users
9.4.3	User authentication for external connections	1. Policy on the selection of authentication methods for external connections commensurate with risk level of asset 2. Dial-back procedures and controls (e.g., dial-back modems) for authenticating users trying to establish a connection to OIT's network from remote locations.	1. ISO17799 provides examples of various types of authentication methods. 2. Dial-back controls could be applied where applicable as commensurate with asset risk level.
9.4.4	Node authentication	Authenticating automatic connections to remote computers	
9.4.5	Remote diagnostic port protection	Protection of diagnostic ports (e.g., dial-up remote diagnostic facility for maintenance engineers)	
9.4.6	Segregation in networks	Divide large network(s) into separate logical network domains using a secure gateway (e.g., firewall) for internal vs external groups, and for different internal groups	
9.4.7	Network connection control	Access control policy for shared networks (e.g., across organizational boundaries) for restricting connection capability of users	
9.5.1	Automatic terminal identification (as part of operating system access control)	Usage of automatic terminal identification to authenticate connections to specific locations and portable equipment	Use operating system software that identifies a terminal attempting access
9.5.2	Terminal log-on procedures	1. System or application identifiers are not displayed until the log-on process has been successfully completed 2. Help messages are not provided during the log-on procedure that would aid an unauthorized user 3. Validation of log-on information occurs at the completion of all input data. If an error arises during log-on, the system does not indicate which part of the data is incorrect. 4. Limit the number of unsuccessful log-on attempts allowed (three is recommended) 5. Limit the maximum and minimum time allowed for the	

ISO 17799 Section	Topic	Controls	Comments
		log-on procedure 6. Upon successful log-on, display date and time of previous successful log-on, and details of any unsuccessful log-on attempts since the last successful log-on	
9.5.5	Use of system utilities (as related to operating system)	1. Segregation of system utilities from application software 2. Authorization for ad hoc use of system utilities 3. Limitation of the availability of system utilities (e.g., for the duration of an authorized change) 4. Logging of all use of system utilities 5. Defining and documenting of authorization levels for system utilities	S-vector can measure the existence of these controls. Policies for these controls would be included in the Information Security Policy Document.
9.5.7	Terminal time-out	Shut down (clear terminal screen and close both application and network sessions) of inactive terminals in high risk locations after a defined period of inactivity to prevent access by unauthorized persons.	
9.5.8	Limitation of connection time	Enforce restrictions on connection times for high-risk applications	Examples of such restrictions include usage of predetermine time slots for batch file transmissions, time period limitations for allowing terminal connections
9.6.2	Sensitive system isolation (as related to application access control)	Identify the sensitivity of an application (e.g., should run on dedicated computer; should only share resources with trusted application systems; no limitations)	
9.7.1 9.7.2	Monitoring System Access & Use	1. Implement event logging (audit logs and recommended items to record) 2. Procedures for reviewing events (i.e., audit logs), to include frequency of review and what risk factors to monitor against 3. Procedure for monitoring and correcting clock synchronization (so that audit logs reflect accurate time)	
9.8	Mobile computing and “teleworking”	Develop a formal policy for mobile computing (i.e., usage of notebooks, palmtops, mobile phones, etc.) that includes various security controls such as: 1. Physical protection 2. Access controls 3. Cryptographic techniques 4. Virus protection	

ISO 17799 Section	Topic	Controls	Comments
		5. Back-ups 6. Audit and security monitoring 7. Training employees on risks associated with mobile computing	
10.1	Security requirements analysis and specification (related to System Development & Maintenance)	Determine, gain agreement on, and document security requirements and controls during requirements phase of a system development project. Include both automated and manual security controls required of the system that are commensurate with the system's security risk.	This would have to be manually validated i.e., whether security requirements are included in design specifications of new systems and system revisions
10.3.1	Policy on the use of cryptographic controls	1. Policy document that contains any or each of the following items (as seen relevant by OA/OIT) 2. General principles towards usage of cryptographic controls a. Policy on when to use encryption b. Strength of encryption (length of key) to use for various levels of desired security 3. Usage of non-repudiation services to resolve disputes involving the use of digital signatures or payments. 4. How the appropriate level of cryptographic protection will be determined 5. Roles and responsibilities 6. Implementation of the policy	Usage of cryptographic controls is based on the risk assessment to determine which applications and data items need this protection, and to what extent.  ISO 17799 recommends using separate keys for encryption and digital signatures.  S-vector can score this component based on the existence of a policy and its inclusion of relevant items (listed in the previous column)
10.3.5.1 10.3.5.2	Key management (related to cryptographic controls)	ISO 17799 contains over 11 items to be included in key management policy – all of which are relevant to OA/OIT and can be included in S-vector. A partial list of the procedural components include: 1. Length of time in which keys are valid 2. Key generation for different types of cryptographic controls and different application 3. Key distribution 4. Recovery of encrypted data in case of lost, compromised, or damaged keys 5. Protection of private, secret, and public keys, as well as if/when to use certificates 6. Physical protection to protect equipment used to generate, store, and archive keys	

ISO 17799 Section	Topic	Controls	Comments
10.4.1	Control of operational software (in industry, also referred to as production software)	<ol style="list-style-type: none"> <li>1. Evidence of successful testing and user acceptance is achieved prior to implementing executable code on an operational system (i.e., on a production server)</li> <li>2. An audit log is maintained of all updates to operational program libraries</li> <li>3. Previous versions of software are retained as a contingency measure</li> <li>4. If possible, operational systems only contain executable code (program libraries are stored separately)</li> </ol>	S-vector can verify the existence of these controls. During an audit, it can be determined if a configuration management or change control policy is in place and actively used. It can also be verified that an audit log exists and is actively maintained of updates to libraries. Etcetera.
10.4.2	Protection of system test data	<ol style="list-style-type: none"> <li>1. If operational data contains personal data, it should be de-personalized before using it for testing.</li> <li>2. Authorization is required/obtained each time operational information is copied to a test application system</li> <li>3. The copying and use of operational information is logged to provide an audit trail</li> <li>4. Operational information is erased from a test application system immediately after the testing is complete</li> </ol>	These controls apply to the common practice of copying operational (production) data over to a test server for use in testing new or modified programs. ISO 17799 recommends treating operational data with the same precaution in a test environment that it would receive in a operational environment.
10.4.3	Access control to program source library		9 controls are recommended for protecting program source code libraries
10.5.1 10.5.2	Change control procedures		<p>ISO 17799 contains a detailed list of recommendations for change control (also known as configuration management) of operational systems. Several of the items would not be easily verifiable using S-vector and may be outside the scope of S-vector.</p> <p>What is relevant from an S-vector perspective is that a formal change control program can facilitate verification of other S-vector procedural components.</p>
10.5.3 10.5.4 10.5.5	Software packages and outsourced software development	<ol style="list-style-type: none"> <li>1. Policies for restricting changes to software packages</li> <li>2. Safeguards against buying software containing Trojan code and covert channels that expose information</li> <li>3. Guidelines for assessing quality of outsourced software development from a security perspective</li> </ol>	

Structural Components

ISO 17799 Section	Topic	Controls	Comments
10.2.2.1	Areas of risk (related to System Development & Maintenance)	Perform validation checks within software code to check: <ol style="list-style-type: none"> <li>1. Use and location of add/delete functions</li> <li>2. Procedures to prevent programs from running in wrong order or after failure of prior processing</li> <li>3. Use of correct programs to recover from failure</li> </ol>	For S-vector applications chosen to perform these checks, the checks can be validated by either a QA tester or configuration management team prior to system deployment – depending on how OA/OIT signs off on a system ready for deployment.
10.2.2.2	Checks and controls (included in program code)	<ol style="list-style-type: none"> <li>1. Reconcile file balances after transaction updates</li> <li>2. Balancing controls to check opening balances against previous closing balances</li> <li>3. Validation of system generated data</li> <li>4. Hash totals of records and files</li> <li>5. Checks to ensure programs are run at correct time</li> <li>6. Checks to ensure programs are run in the correct order and terminate in case of a failure</li> </ol>	The checks to perform depend on the type of application. For example, validating financial balances may only be applicable to PennDOT or licensing applications.  The need for these checks, to include specific data items, are to be documented in the “Security Requirements Analysis and Specification” mentioned in section 10.1 above.  Validation of these checks & controls could be performed as part of the QA process that application software goes through prior to being placed into production.
10.2.3	Message authentication		High-level and incomplete guidelines. Common criteria may provide more specific detail.
10.2.4	Output data validation		High-level and incomplete guidelines. Common criteria may provide more specific detail.

## B - Areas of ISO 17799 not suggested as S-vector components

The following table contains a list of ISO 17799 controls not suggested in the previous section for use by S-vector. The Topics column contains specific or subgroups of controls. Numbers enclosed in parentheses indicate the corresponding ISO 17799 section(s). The Comments column contains a brief description of the control and the reasoning for omitting the control from recommendation. Please keep in mind that both the recommended and omitted controls are suggestions for discussion by the S-vector research team.

Topic	Comments
Half of the information security infrastructure (4.1) area: <ul style="list-style-type: none"> <li>▪ Authorization process for new information processing facilities (4.1.4)</li> <li>▪ Specialist information security advice (4.1.5)</li> <li>▪ Cooperation between organizations, such as law enforcement, regulatory bodies, etc. (4.1.6)</li> <li>▪ Independent review of information security (4.1.7)</li> </ul>	Although 3 subsections of 4.1 are recommended, these 4 subsections of 4.1 are thought to be outside scope of S-vector.
Physical security of facilities & equipment (7.1-7.3)	<p>Covers physical security of information processing facilities, such as the Server Farm. Example controls include locking doors and windows, usage of intruder detection systems, usage of visitor logs, etc. Believe this to be outside the scope of S-vector.</p> <p>The Strawman S-vector Structure mentions physical security. I'm not sure what aspects of physical security are intended for coverage in S-vector. Note that ISO 17799 section 7.2 addresses equipment security, such as power, cabling, etc.</p>
Communications and Operations Management (8)	With the exception of Incident Management Procedures (8.1.3), this ISO 17799 area was not recommended because it is outside the scope of S-vector. The area contains guidelines for operations management, such as capacity planning, backups, and network management. Management controls for email and other forms of information exchange are included.
Business continuity management (11)	Details of business continuity management is outside the scope of S-vector. However, other recommended controls ensure that policies are in place for responding to security incidents.
Compliance (12)	Includes high-level guidelines for compliance with legal requirements such as intellectual property rights, safeguarding organizational records, collection of (legal) evidence, etc. Section 12 also covers "system audit considerations." May be outside the scope of S-vector. Legal requirements can be covered within a security policy document or specified as specific S-vector elements.

## C – Description of SSE-CMM Process Areas

The following table contains a list of all twenty-two process areas (PA) within SSE-CMM. The first eleven PA's are security-related and applicable as S-vector procedural components. All base practices belonging to security-related PA's are provided. The remaining eleven PA's are general systems engineering practices and believed to be outside the scope of an S-vector implementation; therefore, base practices for these PA's are not listed. However, security-related PA's that may address aspects of PA12 - PA22 are provided. The wording of the process areas and base practices are taken directly from SSE-CMM.

SSE-CMM Process Areas	Base Practices	Comments
PA01: Administer Security Controls		SSE-CMM does not provide guidelines or recommendations for the security controls themselves. It deals only with administering security controls that, implicitly, were previously determined. ISO 17799 controls could be employed, while SSE-CMM PA01 is used to establish a management framework for administering those controls.
	BP.01.01 Establish responsibilities and accountability for security controls and communicate them to everyone in the organization	
	BP.01.02 Manage the configuration of system security controls	
	BP.01.03 Manage security awareness, training, and education programs for all users and administrators	
	BP.01.04 Manage periodic maintenance and administration of security services and control mechanisms	This base practice appears to be a catch-all that contains administrative elements (e.g., maintaining logs & reviews), security policy document elements (e.g., descriptions of types of information & media and how they should be managed from a security perspective), and technical control elements (e.g., procedures for identification & authentication, access mediation & control, and key management). No details for specific controls provided.
PA02: Access Impact		SSE-CMM defines impact as the consequence of an unwanted incident, caused either deliberately or accidentally, which affects the assets.
	BP.02.01 Identify, analyze, and prioritize operational, business, or mission capabilities leveraged by the system	This base practice influences the prioritization of risks addressed by security controls.

SSE-CMM Process Areas	Base Practices	Comments
	BP.02.02 Identify and characterize the system assets that support the key operational capabilities or the security objectives of the system	
	BP.02.03 Select the impact metric to be used for this assessment	
	BP.02.04 Identify the relationship between the selected metrics for this assessment and metric conversion factors if required	The result of this base practice is the consolidation of multiple metric systems that are employed across an application – possibly at different levels of abstraction
	BP.02.05 Identify and characterize impacts	
	BP.02.06 Monitor ongoing changes in the impacts	
PA03: Assess Security Risk		This PA focuses on ascertaining risks based on an established understanding of how capabilities & assets (PA02) are vulnerable (PA05) to threats (PA04). Involves identifying & assessing the likelihood of the occurrence of “exposures,” which SSE-CMM defines as the combination of a threat, vulnerability, & impact that could cause significant harm. The goal is find exposures that justify preventive security measures. Does not provide guidelines or recommendations for a risk assessment methodology.
	BP.03.01 Select the methods, techniques, and criteria by which security risks, for the system in a defined environment are analyzed, assessed, and compared	
	BP.03.02 Identify threat/vulnerability/impact triples (exposures)	
	BP.03.03 Assess the risk associated with the occurrence of an exposure	
	BP.03.04 Assess the total uncertainty associated with the risk for the exposure	
	BP.03.05 Order risks by priority	
	BP.03.06 Monitor ongoing changes in the risk spectrum and changes to their characteristics	
PA04: Assess Threat		Recommends developing threat scenarios to more fully understand threat and its impact. This PA does not provide specific recommendations on a threat assessment methodology; however, the base practices provide high-level guidance in this area.
	BP.04.01 Identify applicable threats arising from a natural source	Also estimate likelihood of occurrence.

SSE-CMM Process Areas	Base Practices	Comments
	BP.04.02 Identify applicable threats arising from man-made sources, either accidental or deliberate	Also estimate likelihood of occurrence. A generic “man-made threat database” is suggested as an aid for developing threat scenarios.
	BP.04.03 Identify appropriate units of measure, and applicable ranges, in a specified environment	
	BP.04.04 Assess capability and motivation of threat agent for threats arising from man-made sources	
	BP.04.05 Assess the likelihood of an occurrence of a threat event	
	BP.04.06 Monitor ongoing changes in the threat spectrum and changes to their characteristics	
PA05: Assess Vulnerability		Does not recommend a specific methodology for vulnerability analysis, but does mention some techniques that are used. Part of the analysis involves creating attack scenarios and tests.
	BP.05.01 Select methods, techniques, and criteria by which security system vulnerabilities in a defined environment are identified and characterized	
	BP.05.02 Identify system security vulnerabilities	Software can be used for locating common vulnerabilities. More detailed “penetration testing” is required to uncover uncommon vulnerabilities.
	BP.05.03 Gather data related to the properties of the vulnerabilities	
	BP.05.04 Assess the system vulnerability and aggregate vulnerabilities that result from specific vulnerabilities and combinations of specific vulnerabilities	
	BP.05.05 Monitor ongoing changes in the applicable vulnerabilities and changes to their characteristics	
PA06: Build Assurance Argument		The purpose of this PA is to “clearly convey that the customer’s security needs are met.” Assurance is the level of confidence in system security required by customer.
	BP.06.01 Identify the security assurance objectives	
	BP.06.02 Define a security assurance strategy to address all assurance objectives	
	BP.06.03 Identify and control security assurance evidence	Evidence may be gathered from a database, system logs, test results, etc., and is used to convey assurance that security objectives have been met.

SSE-CMM Process Areas	Base Practices	Comments
	BP.06.04 Perform analysis of security assurance evidence	
	BP.06.05 Provide a security assurance argument that demonstrates the customer's security needs are met	Present objectives and evidence of meeting objectives to user.
PA07: Coordinate Security		The purpose of this PA is to ensure that all relevant parties involved in system security are aware of and involved in security activities.
	BP.07.01 Define security engineering coordination objectives and relationships	
	BP.07.02 Identify coordination mechanisms for security engineering	
	BP.07.03 Facilitate security engineering coordination	
	BP.07.04 Use the identified mechanisms to coordinate decisions and recommendations related to security	
PA08: Monitor Security Posture		This PA includes practices for identifying and reporting breaches or mistakes that could lead to a breach. "Security posture" indicates readiness of system and its environment to handle current threats, vulnerabilities, and any impact to the system and its assets.
	BP.08.01 Analyze event records to determine the cause of an event, how it proceeded, and likely future events	Requires development of event records by creating a composition of various system logs. Event records are then analyzed for security activity. Requires an understanding of which events can be discovered via logs, and which cannot.
	BP.08.02 Monitor changes in threats, vulnerabilities, impacts, risks, and the environment	
	BP.08.03 Identify security relevant incidents	Requires an understanding of types of possible attacks, as well as actions to take when a security incident has occurred. Response plans are developed in this BP, and analysis of incident trends is conducted (e.g., via reports).
	BP.08.04 Monitor the performance and functional effectiveness of security safeguards	
	BP.08.05 Review the security posture of the system to identify necessary changes	Requires a reassessment of the adequacy of current security and the appropriateness of the current level of risk acceptance.
	BP.08.06 Manage the response to security relevant incidents	Requires developing a contingency plan for responding to system disruption due to security events (i.e., attacks). The contingency plan indicates max acceptable period of system downtime, essential system functionality, recovery strategy & plan, and testing & maintaining the plan.

SSE-CMM Process Areas	Base Practices	Comments
	BP.08.07 Ensure that the artifacts related to security monitoring are suitably protected	Establishes a policy for sealing and archiving security-related logs and ensuring that they are complete and valid. The BP also requires specifying a time period for maintaining archives.
PA09: Provide Security Input		Provide security input to support system design, implementation, and maintenance activities.
	BP.09.01 Work with designers, developers, and users to ensure that appropriate parties have a common understanding of security input needs	The security assurance plan developed in PA06 may influence what inputs are needed in order to generate assurance evidence.
	BP.09.02 Determine the security constraints and considerations needed to make informed engineering choices	
	BP.09.03 Identify alternative solutions to security related engineering problems	Alternatives include architecture, design, & implementation solutions.
	BP.09.04 Analyze and prioritize engineering alternatives using security constraints and considerations	
	BP.09.05 Provide security related guidance to other engineering groups	
	BP.09.06 Provide security related guidance to operational system users and administrators	Operational guidance tells users & administrators what must be done to install, configure, operate, & decommission a system in a secure manner.
PA10: Specify Security Needs		The purpose of this PA is to define security objectives & requirements that will meet all legal, policy, and organizational requirements for security. Requirements for each applicable customer group & location must be considered throughout this PA and its related base practices.
	BP.10.01 Gain an understanding of the customer's security needs	
	BP.10.02 Identify laws, policies, standards, external influences and constraints that govern the system	
	BP.10.03 Identify the purpose of the system in order to determine the security context	Purpose is to define the security perimeter, which could be thought of as the scope, context, and environment to which security controls will apply.
	BP.10.04 Capture a high-level security oriented view of the system operation	Develop a high-level security view of the system architecture, procedures, & environment to include information flow, assets, resources, personnel, and physical protection. Also referred to as "security concept of operations."

<b>SSE-CMM Process Areas</b>	<b>Base Practices</b>	<b>Comments</b>
	BP.10.05 Capture high-level goals that define the security of the system	At a minimum, develop security objectives that address system and information availability, accountability, authenticity, confidentiality, integrity, and reliability.
	BP.10.06 Define a consistent set of statements which define the protection to be implemented in the system	
	BP.10.07 Obtain agreement that the specified security meets the customer's needs	Obtain approval of security objectives & requirements and ensure there is an agreed consensus among all relevant parties.
PA11: Verify and Validate Security		Verify & validate that solution meets security requirements. To be performed by a group different than the engineering group that designed, developed, & implemented system.
	BP.11.01 Identify the solution to be verified and validated	
	BP.11.02 Define the approach and level of rigor for verifying and validating each solution	
	BP.11.03 Verify that the solution implements the requirements associated with the previous level of abstraction	
	BP.11.04 Validate the solution by showing that it satisfies the needs associated with the previous level of abstraction, ultimately meeting the customer's operational security needs	
	BP.11.05 Capture the verification and validation results for the other engineering groups	Results should include traceability from security needs to requirements, solution, through to test results.
PA12: Ensure Quality		Adapted from SE-CMM and considered outside the scope of S-vector. Relevant sections of this PA are handled by PA06.
PA13: Manage Configurations		Adapted from SE-CMM and considered outside the scope of S-vector. Relevant sections of this PA are handled by PA01.
PA14: Manage Project Risk		Risk in the SE-CMM context relates to risk associated with completing projects on time & on budget. Risk related to security is addressed in PA03.
PA15: Monitor and Control Technical Effort		Aspects of PA01 and PA08 are used to assign and monitor security-related practices.
PA 16: Plan Technical Effort		This PA addresses estimating technical resources and scheduling activities over the project lifecycle. PA07 handles relevant security-related practices.
PA17: Define Organization's System (or Security) Engineering Process		May be sufficiently handled by PA01.

SSE-CMM Process Areas	Base Practices	Comments
PA18: Improve Organization's System (or Security) Engineering Processes		My impression is that the goals of this PA can be satisfied by increasing the capability level of PA17 (or PA01 if used in lieu of PA01) to 5.
PA19: Mangle Product Line Evolution		Although this PA could be applied to the development of customer-oriented web applications, it is still considered outside the scope of S-vector.
PA20: Manage Systems Engineering Support Environment		This PA is used to build and maintain a technical infrastructure. From a security perspective, this <i>may</i> be accomplished via PA01.
PA21: Provide Ongoing Skills and Knowledge		May be sufficiently handled by PA01.
PA22: Coordinate with Suppliers		Handled by PA07 and by ISO 17799 controls that deal with outsourcing & vendors.

## D – System Security Assessment Method (SSAM) Evaluation Template

For each SSE-CMM process area (PA), the capability level is determined using the following evaluation template:

- PA name and description
- PA goals
- Capability Level 1
  - *Base* practices listed for the given PA. The respondent checks if each BP is performed or not. For those BP's performed, the respondent is requested to state evidence (e.g., document, person, etc.) of BP being performed. Note that each response for Level 1 is per base practice, not the PA as a whole.
- Capability Level 2
  - *Generic* practices listed for achieving Capability Level 2. The generic practices apply to the PA as a whole, not to specific base practices.
- Remaining Capability Levels 3 – 5 assessed using same format as described for Level 2.

## References

- Barton, R., Hery, W., Liu, P. et al, A Scoring Vector for Managing Web Application Security, NSF Full Proposal, Mar 2004.
- Bisson, J., Saint-Germain, R., The BS 7799 / ISO 17799 Standard, White Paper, Callio Technologies, [https://www.callio.com/files/wp\\_iso\\_en.pdf](https://www.callio.com/files/wp_iso_en.pdf)
- C&A Security Risk Analysis Group, The Security Risk Analysis Directory, <http://www.security-risk-analysis.com/>, 2003
- Callio Technologies, Callio Secura 17799: Training for analysts & consultants, [https://www.callio.com/files/17799\\_and\\_secura.ppt](https://www.callio.com/files/17799_and_secura.ppt)
- Carlson, Tom, Information Security Management: Understanding ISO 17799, Lucent Technologies Worldwide Services, Sep 2001
- Carnegie Mellon University (CMU), Concept of Operations for the CMMI, updated Mar 2004, <http://www.sei.cmu.edu/cmmi/background/conops.html>
- Cheetham, C., Ferraiolo, K., The Systems Security Engineering Capability Maturity Model, 3<sup>rd</sup> Combat Symposium, 1998, 1998The\_SSE-CMM.ppt, <http://www.sse-cmm.org/lib/lib.asp>
- EOS, Egyptian Organization for Standardization and Quality Control, [http://www.eos.org.eg/web\\_en/prog/items/w34731.html](http://www.eos.org.eg/web_en/prog/items/w34731.html)
- Gamma Secure Systems, History of BS 7799, <http://www.gammassl.co.uk/bs7799/history.html>
- Hefner, R., Knode, R., Schanken, M., The Systems Security Engineering CMM, Crosstalk, Oct 2000
- Hery, W., Liu, P., Strawman S-vector Structure, 2003, eBusiness Research Center, Penn State University
- International Systems Security Engineering Association (ISSEA), <http://www.issea.org>
- ISO 17799 News – Issue 1, ISO17799 Security Newsletter – Issue 1, <http://www.iso17799-web.com/issue1.htm>, The ISO 17799 Portal
- ISO 17799 News – Issue 2, ISO17799 Security Newsletter – Issue 2, <http://www.iso17799-web.com/issue2.htm>, The ISO 17799 Portal
- ISO 17799 News – Issue 3, ISO17799 Security Newsletter – Issue 3, <http://www.iso17799-web.com/issue3.htm>, The ISO 17799 Portal
- ISO 17799 News – Issue 10, ISO17799 Security Newsletter – Issue 10, <http://www.iso17799-web.com/issue10.htm>, The ISO 17799 Portal
- ISO/IEC 2000, ISO/IEC 17799 Information technology – Code of practice for information security management, Reference number ISO/IEC 17799:2000(E)

Kenning, M.J., Security management standard – ISO 17799/BS 7799, BT Technology Journal, Jul 2001; pp 132

Lucent Technologies, Information Security Management: Understanding ISO 17799, White Paper, Apr 2004, <http://www.lucent.com/knowledge/archives/0,1981,inDocTypeId+115-inPageNumber+1-inByLocation+0-SORT+D,00.html>

National Institute of Standards and Technology's (NIST) Information Technology Laboratory, International Standard ISO/IEC 17799:2000 Code of Practice for Information Security Management Frequently Asked Questions, Nov 2002, [http://sbc.nist.gov/PDF/ISO\\_IEC\\_17799\\_2000\\_Inf\\_Sec\\_Mgmt\\_FAQ.pdf](http://sbc.nist.gov/PDF/ISO_IEC_17799_2000_Inf_Sec_Mgmt_FAQ.pdf)

Pattinson, F., Comparing ISO 17799:2000 with SSE CMM V2, Phi Solutions, Sep 19, 2002, [http://www.phi-solutions.com/documents/ISO17799\\_SSE\\_CMM\\_comparison.pdf](http://www.phi-solutions.com/documents/ISO17799_SSE_CMM_comparison.pdf)

Rees, R., Blum, R., Measuring Security Controls Maturity and Compliance, International Network Services (INS) NetKnowledge Webinar, [http://www.ins.com/knowledge/webseminar\\_archives.asp](http://www.ins.com/knowledge/webseminar_archives.asp), Apr 2004

SECAT LLC, Overview of the Systems Security Engineering Capability Maturity Model (SSE-CMM), <http://www.secat.com>, 1996

Small, R., Brykczynski, B., Using ISO 17799, A Code of Practice for Information Security Management, to Best Advantage, Software Productivity Consortium, Presentation at RSA 2003, <http://www.software.org/pub/externalpapers/archives.asp>, Apr 14, 2003

Symantec Enterprise Solutions, The Emerging Global Security Standard: ISO 17799, Apr 2, 2002, Article ID: 1261

Symantec Enterprise Solutions, A Definitive Introduction to Information Security Policies, Standards and Policies, Jul 16, 2002, Article ID: 1155

Symantec Enterprise Solutions, A Definitive Introduction to Information Security Policies, Standards and Policies (Part 2), Feb 5, 2002, Article ID: 1165

Symantec Enterprise Solutions, A Definitive Introduction to Information Security Policies, Standards and Policies (Part 3), Feb 12, 2002, Article ID: 1179

SSE-CMM Project, SSE-CMM Appraisal Method Description, (SSAM), Version 2.0, Apr 19, 1999, <http://www.sse-cmm.org/org/org.asp>, SSAM.pdf

SSE-CMM Project, Systems Security Engineering Capability Maturity Model SSE-CMM Model Description Document, Version 3.0, Jun 15, 2003

Thiagarajan V., Information Security Management BS 7799.2:2002 Audit Check List for SANS, Jun 8, 2003