System Security Capability Assessment Model Development and Application

Joseph J. Simpson
System Concepts, LLC
6400 32nd Avenue N.W., #9
Seattle, WA 98107
206-781-7089
jjs-sbw@eskimo.com

Dr. Barbara Endicott-Popovsky, Director
Center for Information Assurance and Cybersecurity
University of Washington
4311 11th Avenue N.E., Suite 400
Box 354985
Seattle, Washington 98105
206-284-6123
endicott@u.washington.edu

Abstract. The INCOSE Systems Engineering Capability Assessment Model (SECAM) has been adapted to apply to the system security domain. Service organizations that do not produce an industrial manufactured product are the initial target of this new variation of capability assessment model. The primary goal of this work is the deployment of an adaptive set of organizational security assessment tools that provide the basis for controlled, structured organizational improvement of the existing security context. A new quick look assessment method is also presented to help an organization minimize the cost and time associated with this type of activity.

Introduction

System security is recognized as a critical area in systems development and operations. The INCOSE Systems Engineering Capability Assessment Model (SECAM) is modified, and a new derivative work is developed that applies directly to the evaluation of an organizations' ability to consistently operate in a secure and appropriate manner. This activity is facilitated by the open document license that covers both parts of the INCOSE SECAM as well as the general focus of the SECAM on organizational staged evaluation and organizational activity improvement. The basic form and function of the SECAM is evaluated to identify the areas that need to be modified to support the design, development and deployment of a System Security Capability Assessment Model (SSCAM). Further, a SSCAM Quick Look (QL) model is designed to determine if an organization is in a state where a complete SSCAM assessment method could be effectively applied.

Organizations have been separated into three general types: 1) organizations that produce a manufactured industrial product and/or service as a vender to a customer, 2) organizations that produce a manufactured industrial product and/or service as well as manage an industrial process for the customer, 3) organizations that do not produce a manufactured industrial product but are required to appropriately and securely manage data and/or information that is received, produced and/or acquired during the course of business with their customer. Some general examples of the third type of organizational activity are heath care, schools, banking, insurance, public utility, and

critical infrastructure operation.

SECAM Purpose and Structure

The INCOSE Capability Assessment Working Group (CAWG) started working on a formal method and technique to support the improvement of systems engineering capability in large industrial organizations in the early 1990's. As stated in the published SECAM document, the focus of the model is to assess an organizations systems engineering capability for integrated systems and integrated product and process development (IPPD) teams and determine areas for improvement. The organization's manufactured products are produced for the customer using the organization's structure, processes, manufacturing facilities and support systems that are reviewed as part of the SECAM assessment and evaluation. Further, the collaborative, open manner in which INCOSE developed the SECAM provides the basis upon which derivative works can be based. The SECAM measures system engineering capability performance based on six areas: people, processes, technology, resources, control and agility. This focus on a larger set of organizational features that go beyond the product development process, provides a foundation for the modification of the SECAM so it can be applied to organizational activities that do not produce a manufactured industrial product.

The SECAM model is divided into three general sections: management, organization and systems engineering. The management section is further decomposed into, planning, tracking and oversight, subcontract management, inter-group coordination, configuration management, quality management, risk management, and data management. The organizational section is further divided into, process management and improvement, competency development, technology management, as well as environment and tool support. The system engineering section is further decomposed into: system concept development, requirements and functional analysis, system design, integrated engineering analysis, system integration, system verification and system validation. Only the system engineering area would need major modification to translate the SECAM to the domain of system security engineering and operations. Other areas of the SECAM would need some minor changes to properly support and focus activity on the security engineering and operational aspects of an organization. This version of the SSCAM is focused on organizations that do not produce a manufactured industrial product or service and therefore do not have a set of customer requirements that drive the organizational activities. The controlling organizational system security operational requirements are levied by laws, regulations, contractual obligations as well as the organizations security posture and domain of operation. Figure 1 shows the relationship between the SECAM and SSCAM.

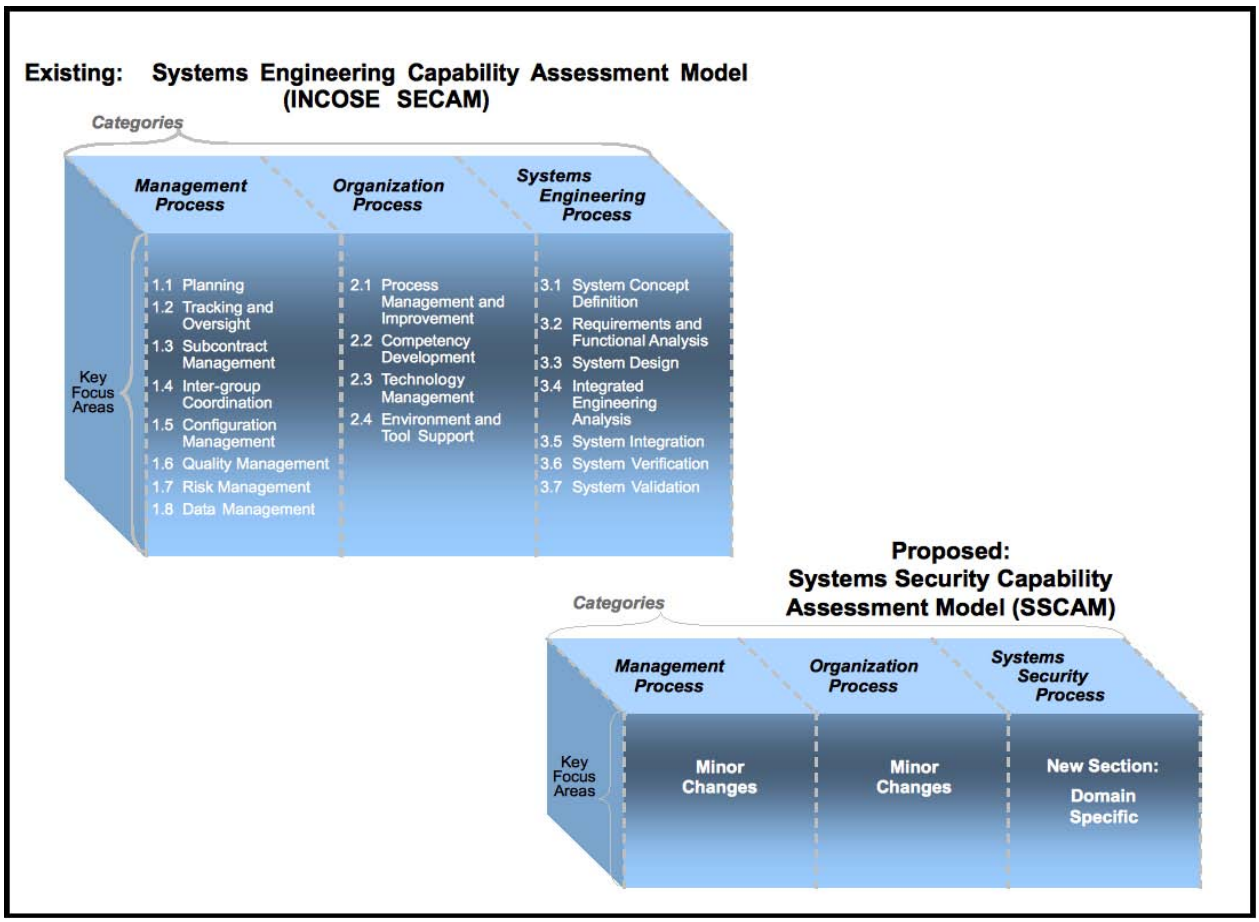

Figure 1. Relationship between SECAM and SSCAM

SECAM Modification

The SECAM is divided into three broad categories, management, organization, and systems engineering. The SSCAM maintains the first two categories and changes the third category to security engineering and operations. The focus of the management and organizational categories are changed from systems engineering to security engineering. All of the changes in categories one and two are considered to be very low impact. However, there are substantial changes in the third category that have a high impact on the model content and application. These substantial changes are driven by the source and nature of the operational security requirements.

The eight SSCAM management subcategories are constructed to apply to every operational domain area without modification. The four SSCAM organizational subcategories are also designed to apply equally well to any operational domain without modification. Therefore only the third category, security engineering and operations will need to be adjusted for each individual domain of application. This domain specific model adjustment requires a model with two levels: a global level and a local level. The global level model is designed to cover all domain types and address categories one and two in a common manner while at the same time providing a model mechanism to allow the insertion of domain specific model components for category three evaluations and assessments. A primary aspect of the global level model is the identification, definition and enumeration of all allowable application domain areas. Figure 2 shows the

relationship between the global level model and local level model components.

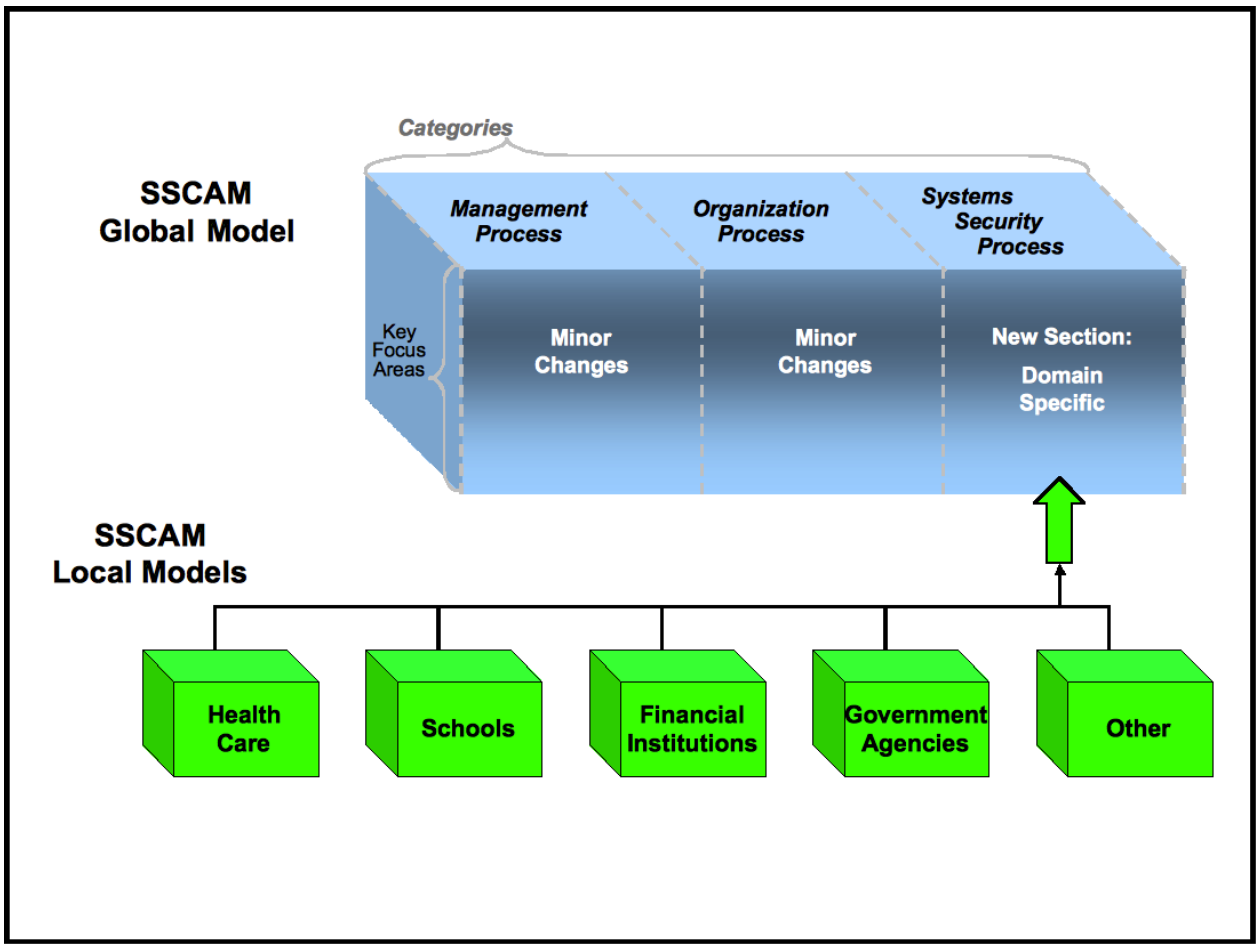

Figure 2. Relationship between Global-Level Model and Local-Level Model Components

The local level model, or domain model level, has specific objectives and requirements that are valid for the selected application domain. Each local level model will be developed by a group of industry and government experts that are recognized for their depth of knowledge in the selected security application area. The domain specific security requirements are organized around the following areas: security mission function analysis; security functional analysis; security requirements analysis; security operational design; security operational integration; and security operational test and evaluation. This standard format for organizing each of the identified domain areas provides a common template that will increase the ability of security professionals to communicate in a more precise and focused manner.

SECAM Assessment Method Structure

In addition to the INCOSE SECAM the CAWG also produced a SECAM assessment method that is used to evaluate an organization using the SECAM. The assessment method is used in combination with the SECAM to measure an organization's current state of systems engineering capability, to identify problem areas, and to provide a structured basis for the improvement of systems engineering capability. The assessment method is a structured organizational audit

conducted by a team of trained individuals that have been invited and authorized to evaluate the organization. The SECAM assessment method consists of the following steps: select the organization to assess, obtain management approval for the assessment, plan the assessment, conduct the assessment, tabulate assessment results, and record and report assessment results. The assessment process provides areas and techniques used to tailor the assessment to fit a specific organization and/or specific assessment purpose. This flexibility is a design feature of the assessment method that supports the flexible, adaptive application of the SECAM or a similar type of capability assessment model.

The SECAM assessment method does not contain a formal "quick look" type of activity or model mode. One reason for the lack of a quick look assessment mode in the SECAM, is based on the fact that the SECAM is a self-improvement assessment model and not a contractual, audit assessment. Individuals in the organization being assessed are assumed to have performed an informal assessment, and determined that a more detailed SECAM effort would provide valuable information for the organization.

SSCAM Purpose, Structure and Organizational Support

The SSCAM is designed to assess and evaluate an organizations security operations capability. This capability rating is determined from the SSCAM rating process that covers three components: management, organization and system security. Both the SSCAM management and organization components are designed to be applied to organizations that operate in any specific domain area. However, the content of the systems security component must be developed for and tailored to each domain of application due to the varying legal, operational, and functional requirements associated with each domain. The SSCAM is divided into two model levels to facilitate the proper model content development, control and application. The first level of the model is the global model level that covers the management and organization components as well as enumerates all of the allowable local level model domains. The second level of the model, the local level, consists of a series of domain specific components that apply to specific domains of security operation. The local level models can be viewed as interchangeable model components or "plug-ins" that are designed to be independently designed and developed in a manner that fits the local level model interface that is defined by the global level model.

The power and effectiveness of the SSCAM is directly related to the standing, type and nature of the individuals and organizations that are charged with creation and application of the SSCAM. Given this fact, the global model development and utilization must be guided by a Global Model Advisory Board (GMAB) that is made up of three types of members. These member types are individual security experts, government organization representatives, and private corporation representatives. The GMAB membership for individual security experts is based on the value of their contribution to the global model as well as their relative standing as rated by the organizational members of the GMAB. The GMAB membership is based on organizational interest, area of operation and the payment of a membership fee. The GMAB fee structure is a necessary component that is required to fund the detailed design, development, management and application of the SSCAM.

Each local level model is associated with a specific domain of application and is also developed under the guidance of a Local Model Advisory Board (LMAB). Similar to the GMAB structure, the LMAB is made up of individual security experts, governmental organizations and private corporations. Individual security expert membership is based on the value of their contributions to

the local model as well as their relative standing as rated by the LMAB organizational members. The interface between the global and local model is determined by the global level organization and represents an abstract model interface that all domain models can use to support their specific activities.

The SSCAM Quick Look (QL) approach is used to determine the proper SSCAM local level model component to assign to the organization under review as well as to evaluate the effectiveness of applying the complete SSCAM to the selected organization. If an organization does not have processes, policies and directives that support the implementation of appropriate security practices, then it may not be an effective use of company resources to conduct a complete SSCAM assessment. The SSCAM QL is designed to determine if the application of the complete SSCAM would be advisable.

SSCAM Quick Look Concepts

The SSCAM QL is designed to evaluate an organizations capability to appropriately handle information security issues encountered during the normal course of business. Three general concepts are used as the foundation of the SSCAM Quick Look Model (QLM): 1) the context within which business is conducted; 2) organization structure and type; and 3) process development and operational control. Each of these components is developed in more detail in the following sections.

Organizational Operational Context. The operational context is viewed as the source of laws, regulations and contractual obligations that impact and help define the system security features, processes and mechanisms that must be implemented by the organization. These contextual obligations must be properly addressed by the organization. Key Contextual Activities (**KCA**) that focus on this contextual relationship are:

KCA 1- Clearly understand current contextual obligations
KCA 2- Monitor changes in the current context
KCA 3- Adapt to changes in the current context

These three key contextual activities are considered the minimum set of actions that an organization would have to perform to maintain awareness of contextual security requirements and obligations.

Organizational Structure and Type. The organizational structure is viewed as the controlling authority that is responsible to assure that the organization successfully meets all of its system security related requirements and obligations. Key Organizational Activities (**KOA**) that focus on the organizational control and accomplishment of the system security requirements are:

KOA 1- Establish and enforce clear lines of Information Assurance and Cyber Security (IACS) responsibility and authority
KOA 2- Plan, monitor and control IACS activities and processes
KOA 3- Properly fund and provide adequate resources for IACS activities and processes

These three key organizational activities are considered the minimum set of actions an organization would have to perform to adequately implement effective system security.

Process Development and Operational Control. The process development and operational control mechanisms are used by the organization to adequately address the system security

requirements that are levied by the operational context. Key Development Activities (**KDA**) that focus on the establishment and maintenance of robust organizational processes are:

KDA 1- Process requirements identification
KDA 2- Process design and deployment
KDA 3- Process management and improvement

These three key process development activities are considered the minimum set of actions needed to be performed by an organization to establish an adequate system security process structure.

SSCAM Quick Look Structure

The SSCAM QL structure is formed as a hierarchy of related concepts and artifacts that, taken as a whole, provide an effective approach to the evaluation of organizational system security capability. The top of the conceptual hierarchy is populated by a single system capability concept that can have a range of alpha values: A, B, C, D, or E. The alpha values are used to make a clear distinction between the SSCAM QLM and outputs or rating from any other type of capability assessment model. The top level capability concept is composed of the three key organizational activities listed above: key contextual activities, key organizational activities, and key development activities. Each of the three key activity areas is composed of process categories. The process categories are composed of key focus areas. Each key focus area is evaluated using a structured set of questions organized by attributes and capability level. The SSCAM QL question set is similar to the question set that is used in more detailed SSCAM evaluations, however, they are used for scoping the follow on assessment activities and are therefore more abstract. See Figure 3 for an overview of the SSCAM QLM structure and top level capability concept.

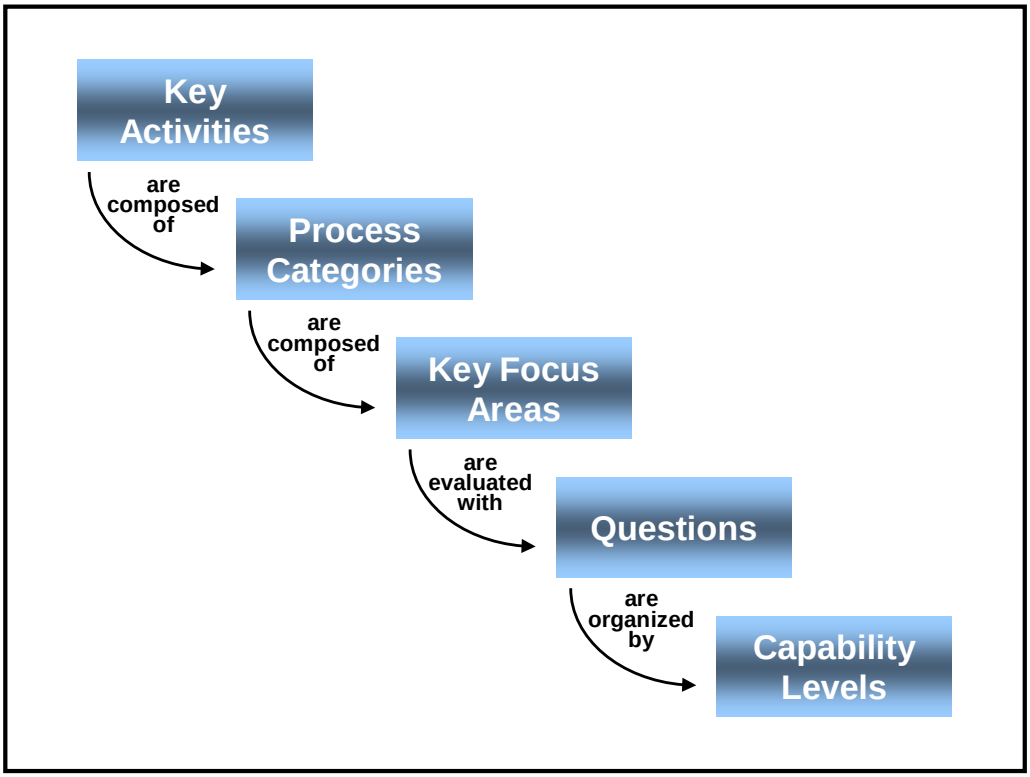

Figure 3. Overview of SSCAM QLM Structure.

SSCAM Quick Look Assessment Method

The SSCAM QL model and the SSCAM QL assessment method are both necessary to conduct an effective SSCAM QL assessment. When applied to a specific organization, the evaluation is called a Security Quick Look Assessment (SQLA). The SQLA is a structured, organized activity that is conducted to achieve the following goals (**G**):

G1 – Measure an organizations system security awareness and capability
G2 – Identify and document system security problem areas
G3 – Provide a baseline analysis that is the foundation for growth in system security capability.

The SSCAM QL assessment approach (**A**) has the following components:

A1 – SSCAM QL Assessment Method Overview
A2 – SSCAM QL Assessment Method Activities
A3 – SSCAM QL Assessment Method On-Site Planning Templates
A4 – SSCAM QLM Questionnaire
A5 – Exploratory Questions
A6 – Heuristic Scoring Method and Template
A7 – Presentation Templates
A8 – Assessment Survey

The SSCAM QL assessment method overview is the beginning step of the SQLA (Figure 4).

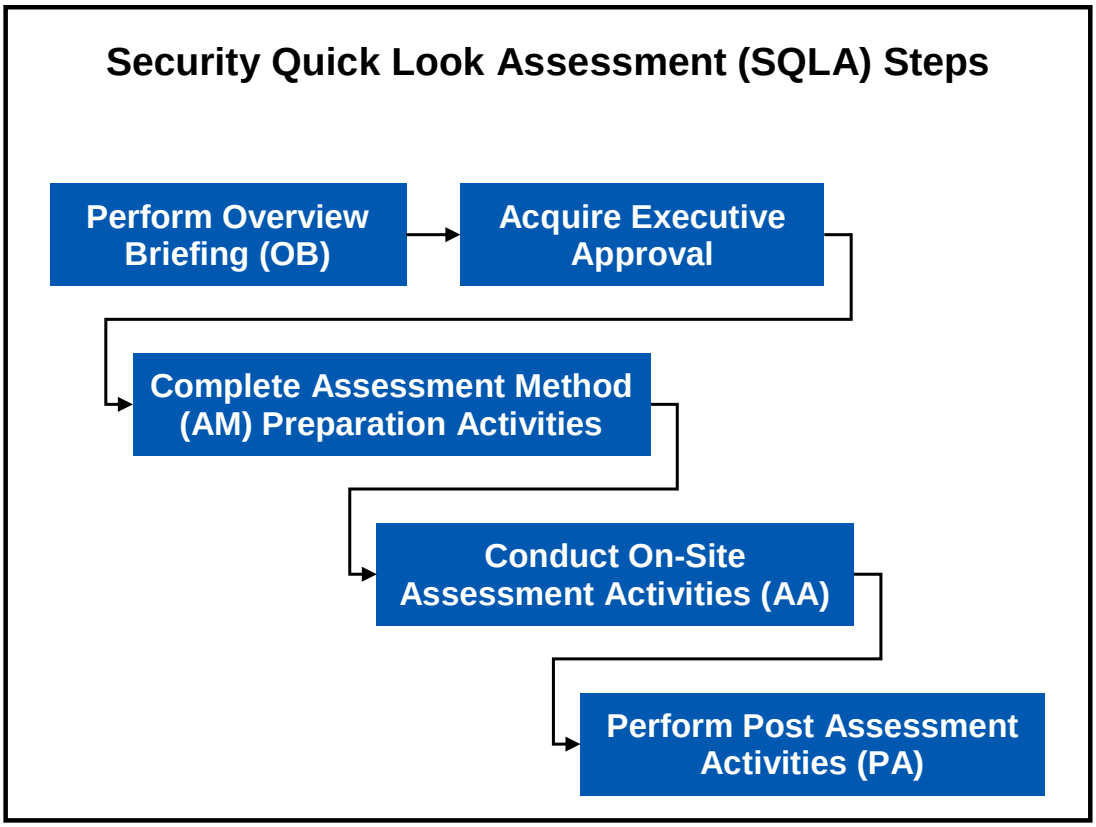

Figure 4. Steps of the SQLA

There are two important and distinct objectives associated with this beginning step: **1) inform senior management about the SQLA process and the associated benefits, and 2) obtain organizational commitment and support to conduct a SQLA.** This is a very important step and must be successfully completed before the SQLA can begin. The SSCAM QL overview briefing (OB) contains the following items:

OB1 – *Assessment Principles and Purpose*
- The quality of the assessment determines the quality of the security processing
- That which is measured, if broken, can be fixed, replaced and/or improved
- Implements a repeatable, structured evaluation and assessment mode

OB2 – *Assessment Conduct Guidelines*
- Emphasize openness and honesty
- Stress the confidentiality of the activity

OB3 – *Assessment Outcomes and Products*
- Identification of strengths and weaknesses
- Statement of findings supported by assessment evidence
- Scoring of each model component area
- Basis for improved security and security processes within the organization

OB4 – *Propose an assessment schedule for executive approval*

OB5 – *Seek positive executive approval for the assessment activity*

OB6 – *Proceed only after receiving positive executive support that has been clearly communicated to the organization*.

After the completion of the SSCAM QL overview briefing and the acquisition of executive approval for the SQLA assessment activity, the assessment preparation activities are initiated. The SQLA assessment method (**AM**) preparation activities are:

AM1- *Form an SQLA Planning Team*
- Identify planning team participants
- Explain the assessment purpose and value of output products
- Review and tailor standard activity descriptions
- Distribute, review and tailor SSCAM QLM Questionnaire
- Identify and assign tasks
- Conduct a question and answer period
- Record lessons learned and other improvement ideas

AM2 – *Characterize the Organization to be Assessed*
- Document the organizational business context
- Develop or obtain a current organization chart
- Document the relationships between the organizational components
- Document the size and function of each organizational component
- Identify key individuals within the organization
- Determine where system security activities are being performed
- Validate and verify the collected and developed information with executive management
- Record lessons learned and other improvement ideas

AM3 – *Develop an Organizational Assessment Strategy*
- Define goal statements for the SQLA
- Define and develop a data gathering strategy based on SQLA goals

Select and tailor, as necessary, the data gathering tools
Document the SQLA assessment strategy and obtain management concurrence
Identify and train assessment team members, as necessary
Identify SQLA assessment participants
Record lessons learned and other improvement ideas

AM4 – *Prepare a SQLA Assessment Draft Action Plan*
Document current organizational security conditions
Record SQLA purpose, goals and scope
Document SQLA participants
Prepare detailed schedule
Outline content and form of SQLA assessment results
Outline content of a follow-up action plan

AM5 – *Provide SQLA Assessment Orientation*
Management opening remarks and support communication
Provide SQLA pre-assessment briefing
Introduce SQLA assessment team
Answer questions and concerns
Record lessons learned and other improvement ideas

AM6 – *Tabulate Questionnaire Data (Practice Set)*
Transcribe Questionnaire responses and tally results
Evaluate responses and calculate metrics
Distribute copies of final data to each team member
Record lessons learned and other improvement ideas

After the SQLA assessment preparation activities are completed, the on-site SQLA assessment activities are conducted. The SQLA assessment activities (**AA**) are:

AA1 – *Conduct SQLA Opening Meeting*
Senior management remarks
SQLA assessment kick-off briefing
Question and answer session
Record lessons learned and other improvement ideas

AA2 – *Prepare SQLA Assessment Team*
Explain goals, products and objects of the SQLA assessment
Provide detailed review of SQLA assessment steps
Review the SQLA assessment questionnaire and responses
Review SQLA assessment schedule
Properly dispose of base input materials
Conduct question and answer period
Record lessons learned and other improvement ideas

AA3 – *Conduct Individual Interviews*
Introduce individual to be interviewed and assessment team members
Explain session purpose
Establish confidentiality rules
Cover the SQLA assessment exploratory questions
Communicate the time and place for the issues review and draft findings report
End interview
Record lessons learned and other improvement ideas

AA4 – *Conduct Group Discussion*
Introduce the discussion topic
Communicate meeting rules
Introduce group members
Repeat confidentiality rules
Conduct group discussion, as necessary
Communicate the time and place for the issues review and draft findings report
End group discussion
Record lessons learned and other improvement ideas

AA5 – *Summarize Issues and Outcomes*
SQLA assessment team members create issues list
Focus issues into individual categories
Prepare issues list for presentation to individual participants
Use SQLA assessment matrix to identify capability score

AA6 – *Review Issues with Individual Participants*
Introduce meeting purpose and structure
SQLA assessment leader reviews each issue list with the individual participants
All significant and/or outstanding issues are noted
SQLA assessment team members record the dialog about the significant issues
Remind the individual participants of the time and place of the draft finding report
End issues review
Record lessons learned and other improvement ideas

AA7 – *Develop Findings*
Identify a common theme in the findings
Group issues into theme groups
Refine the issue groups by adding functional attributes, causes and consequences
Create draft wording for final briefing
Complete a draft of the Final Findings Presentation
Record lessons learned and other improvement ideas

AA8 – *Present Draft Findings to the Individuals and Group Participants*
Welcome participants and present the outline of the presentation
Repeat the confidentiality rules
Present each group outcome
Present each finding and solicit comments
Record comments and concerns
Thanks participants and end the presentation
Use the group feed back to adjust findings
Record lessons learned and other improvement ideas

AA9 – *Review Comments and Findings*
Evaluate each finding
Discuss impact of each finding
Discuss next steps, including a plan and schedule
Record lessons learned and other improvement ideas

AA10 – *Management Final Findings Presentation*
Welcome participants and outline presentation
Repeat confidentiality rules

Make final presentation
Solicit questions, concerns and comments
Thank all participants
Record lessons learned and other improvement ideas

AA11 – *Summarize Lessons Learned*
Review each recorded issue
Determine if the SQLA should be adjusted
Determine if the SQLA tools could be improved
Communicate the improvement finding to the SQLA team

After the completion of the SQLA assessment the SQLA post-assessment phase activities are performed. The SQLA post-assessment activities (**PA**) consist of:

PA1 – *Document the SQLA Assessment Results*
Prepare final report data analysis
Generate SQLA assessment final report, including
Questionnaire summary
Final findings
Significant findings
General comments and recommendations

PA2 – *Complete SQLA Process Improvement Action Plan*
Identify areas for security improvement
Evaluate specific security components that are subject to change
Formulate action plan
Propose security action plan for funding and implementation

PA3 – *Execute the Security Improvement Action Plan*
Review action plan and implementation schedule
Track progress to schedule and budget
Create plan for future assessments and evaluations

SQLA assessment activities are accomplished through the use of templates and questions that have been tailored through the process for the specific assessment at hand.

SQLA Templates and Questions

The SQLA planning templates consist of a standard set of schedule and activity templates used to organize and track the SQLA tasks and activities. These planning templates (**PT**) consist of:

PT1 – Work Breakdown Structure
PT2 – SQLA schedule
PT3 – Resource assignment and allocation

The SQLA data gathering tools consist of two types of question lists. The first question list is the standard SQLA question list that addresses the three key activities and their component processes. The standard question list is distributed to identified participants who score the questions as individuals. The second set of SQLA questions is the set of exploratory questions that are used to guide and focus group discussions. The SQLA assessment adds questions to determine the extent to which an organization engages in each of the three key areas: operational context, structure and type, and process development and operational control. These questions are listed next organized by areas and sub-areas.

Organizational Operational Context. The operational context is viewed as the source of laws, regulations and contractual obligations that impact and help define the system security features, processes and mechanisms that must be implemented by the organization. These contextual obligations must be properly addressed by the organization. The questions (**Q**) associated with the key contextual activities (**KCA**) areas and sub-areas are listed next.

KCA 1- *Clearly understand current contextual obligations*

- **KCA 1.Q1** – Does an informal business contextual statement exist?
- **KCA 1.Q2** – Does a formal business context statement exist?
- **KCA 1.Q3** – Has an individual been selected as a focal point the context area?
- **KCA 1.Q4** – Has the organization identified with specific groups that define the context?

KCA 2- *Monitor changes in the current context*

- **KCA 2.Q1** – Does the organization have an informal understanding of the contextual baseline?
- **KCA 2.Q2** – Does the organization have a formal understanding of the contextual baseline?
- **KCA 2.Q3** – Has an individual been selected to monitor the context changes?
- **KCA 2.Q4** – Has the organization associated with groups that monitor context changes?

KCA 3- *Adapt to changes in the current context*

- **KCA 3.Q1** – Does an informal organizational mechanism exist to adapt to contextual changes?
- **KCA 3.Q2** – Does a formal organizational mechanism exit to adapt to contextual changes?
- **KCA 3.Q3** – Has an individual been selected to monitor organizational changes?
- **KCA 3.Q4** – Has the organization associated with groups that monitor organizational changes?

Organizational Structure and Type. The organizational structure is viewed as the controlling authority that is responsible to assure that the organization successfully meets all of its system security related requirements and obligations. These organizational structure responsibilities must be properly addressed and designed to be effective. The questions associated with the key organizational structure and type activities (**KOA**) areas and sub-areas are listed next.

KOA 1- *Establish and enforce clear lines of IACS responsibility and authority*

- **KOA 1.Q1** – Does an informal understanding of IACS responsibilities exist?
- **KOA 1.Q2** – Does a formal understanding of IACS responsibilities exist?
- **KOA 1.Q3** – Have individual IACS responsibility and authority been assigned?
- **KOA 1.Q4** – Are individual IACS roles assigned according to accepted industry practice?

KOA 2- *Plan, monitor and control IACS activities and processes*

- **KOA 2.Q1** – Do informal IACS planning and control activities exist?
- **KOA 2.Q2** – Do formal IACS planning and control processes exist?
- **KOA 2.Q3** – Is an individual responsible for the IACS planning and control process?
- **KOA 2.Q4** – Are planning and control processes aligned with accepted industry practice?

KOA 3- *Properly fund and resource IACS activities and processes*

- **KOA 3.Q1** – Do informal IACS funding and resource practices exist?
- **KOA 3.Q2** – Do formal IACS funding and resource allocation processes exist?
- **KOA 3.Q3** – Is an individual responsible for the IACS funding and resource allocation process?

KOA 3.Q4 – Are IACS funding and resource practices aligned with accepted industry practice?

Process Development and Operational Control. The process development and operational control mechanisms are used by the organization to adequately address the system security requirements that are levied by the operational context. Key development activities (**KDA**) must be focused on the establishment and maintenance of robust organizational processes that provide the desired level of operational system security. The questions associated with the KDA area and sub-areas are listed next.

KDA 1- *Process requirements identification*

KDA 1.Q1 – Has an informal requirements identification process been established?
KDA 1.Q2 – Has a formal requirements identification process been established?
KDA 1.Q3 – Is an individual responsible for the requirements identification process?
KDA 1.Q4 – Is the requirements identification process aligned with industry practice?

KDA 2- *Process design and deployment*

KDA 2.Q1 – Has an informal design and development process been established?
KDA 2.Q2 – Has a formal design and development process been established?
KDA 2.Q3 – Is an individual responsible for the design and development process?
KDA 2.Q4 – Is the design and development process aligned with industry practice?

KDA 3- *Process management and improvement*

KDA 3.Q1 – Has an informal process management and improvement activity been established?
KDA 3.Q2 – Has a formal process management and improvement activity been established?
KDA 3.Q3 – Is a person responsible for the process management and improvement activity?
KDA 3.Q4 – Is the management and improvement activity aligned with industry practice?

A SQLA assessment activity could be completed after the questions listed above have been answered. If the assessment showed that the organization had little or no processes coupled with an inadequate understanding of the security context, then it would provide little value to continue the SSCAM assessment activity which would focus more tightly on process and organization control of processes. However, if the SQLA assessment activity indicates that the organization has basic processes in place indicating a general understanding of the security context, then proceeding to the next set of more detailed SSCAM activities may indeed provide added value.

SSCAM Application

As computer based communications coupled with computer augmented operations become more wide spread in all industries, the need for a clear, well-defined system security model grows to address the data and information interdependency spawned by the spread of these communication technologies. The output from a SSCAM activity could be used as input to a structured evaluation technique that evaluates the most effective methods to address any indicated security short falls found in the SSCAM QL or SSCAM process assessments. The secure adaptive response potential (SARP) metric was developed to directly support this type of management decision making (Simpson 2008).

In the specific domain of critical infrastructure and electric utility security a capability maturity

model was developed that covered all three areas of people, processes and technology. While the critical infrastructure capability maturity model CI-CMM was based on the Carnegie Mellon Software Engineering Institute Capability Maturity Model (SEI-CMM) the focus of the CI-CMM application is stated as security process improvement and not evaluation for government contracts. Further the CI-CMM was viewed as applicable to many industries in the critical infrastructure domain including; water, natural gas, oil, and transportation (Endicott 2005).

The Federal Aviation Administration (FAA) and the United States Department of Defense (DOD) sponsored the development of a security and safety extension of the current Integrated Capability Maturity Model (iCMM). These extensions were designed to be applied in four basic areas: evaluation of supplier components and services, operational and production environment evaluation, program level audits, and safety and security strategic planning evaluation (Ibrahim 2007).

The continued interest in the application of a formal, structured model for security assessment and evaluation highlights the unfulfilled need for a robust assessment model that can be applied across industrial domains and practices. The SSCAM and SSCAM QL assessment methods detailed in this paper provide the basis for the integration and effective application of security assessment methods to almost any operational domain.

Summary and Conclusions

A robust system security assessment method has been developed and presented in this paper. The constant, dynamic nature of security threats dictated that the model must have a global and local level as well as a direct tie to a supporting organization. The role of the supporting organization is to assure the model is properly designed, developed and applied. This organizational role is constant and dynamic to match the constant and dynamic threat environment.

More research and effort is needed to identify the proper membership for the GMAB, the LMABs, and the proper allocation of local level domain models. However, once this organizational structure has been established, these advisory boards can start to coordinate and direct the model development and application. Also, further research is needed to establish, document and encode the security community's view of the local domain models.

This work is based directly on the work products produced by INCOSE members and demonstrates the strong, continuing technical value provided by INCOSE members who share their accumulated technical management expertise by developing the open work products.

References

Endicott-Popovsky, B. and Lockwood, D. L., 2005. Deriving a capability maturity model for electric utility security assessment. *Academy of Information and Management Sciences Journal* 8 (1).

Ibrahim, 2007. Harmonization of Safety and Security Standards. INSIGHT 10 (2): 37-39. Seattle: INCOSE.

INCOSE 1996. Systems Engineering Capability Assessment Model, Version 1.50a, Document Number INCOSE-TP-1996-002-01. Seattle: INCOSE.

INCOSE 1997. Systems Engineering Capability Assessment Model Assessment Method, Version

1.50. Seattle: INCOSE

Simpson, J. J., Dagli, C., and Miller, A., 2008. Secure Adaptive Response Potential (SARP): A System Security Metric. In Proceedings of the Eighteenth Annual International Symposium of International Council on Systems Engineering (Utrecht, The Netherlands). Seattle: INCOSE.

Biography

Joseph J. Simpson's experience and interests are focused in the area of complex systems, system science, systems thinking and systems management. Joseph has professional experience in several domain areas including environmental restoration, information systems, systems security, aerospace and defense. His current activities and research interests are associated with complex systems modeling, evolutionary programming, the development of a systems engineering language, and organizational assessment and improvement.

Barbara Endicott-Popovsky, Ph.D., is the Director for the Center of Information Assurance and Cybersecurity at the University of Washington, designated by the NSA as a Center for Academic Excellence in Information Assurance Education and Research. She holds a joint faculty appointment with the Information School and the Computer Science Department at the University of Washington at Tacoma, following a 20-year industry career marked by executive and consulting positions in IT architecture and project management. Her research interests include enterprise-wide information systems security and compliance management, forensic-ready networks, the science of digital forensics and secure coding practices. Barbara earned her Ph.D. in Computer Science/Computer Security from the University of Idaho (2007), and holds a Masters of Science in Information Systems Engineering from Seattle Pacific University (1987), a Masters in Business Administration from the University of Washington (1985) and a Bachelor of Arts from the University of Pittsburgh (1967).