System Security Capability Assessment Model Development and Application

Joseph J Simpson, System Concepts, LLC
Dr. Barbara Endicott-Popovsky, University of WA

July 12, 2010

Foreword

Comments, questions, and suggestions related to this presentation are welcome, and may be addressed to:

Joseph J Simpson
jjs-sbw@eskimo.com

Dr. Barbara Endicott-Popovsky
endicott@u.washington.edu

Preface

For twenty years, the International Council on Systems Engineering (INCOSE) has provided a focus and forum for systems engineering professionals to learn, share and create systems engineering products.

- The INCOSE Capability Assessment Working Group created the Systems Engineering Capability Assessment Model Version 1.5 in 1996.
- Copyright 1996 by INCOSE: This work is a collaboration effort of the members of the INTERNATIONAL COUNCIL ON SYSTEMS ENGINEERING (INCOSE). Permission to reproduce this product and to prepare derivative works from this product is granted royalty-free provided this copyright notice is included with all reproductions and derivative works.

Overview

SECAM Purpose and Structure

SECAM Modification

SECAM Assessment Method Structure

SSCAM Purpose, Structure and Organizational Support

SSCAM Quick Look Concepts

SSCAM Quick Look Structure

SSCAM Quick Look Assessment Method

SQLA Templates and Questions

Summary and Conclusions

SECAM Purpose and Structure

SECAM Purpose – formal method and technique to improve the systems engineering capability of large organizations

SECAM Focus is on on integrated product and process development teams

SECAM systems engineering capability is measured by focusing on the following areas:

- People
- Processes
- Technology
- Resources
- Control
- Agility

SECAM Assessment Method Structure

INCOSE CAWG produced the SECAM assessment method to support the evaluation of an organization.

Provides a structured approach to:

- Measure organization's SE capability
- Identify problem areas
- Provide basis for SE capability improvement

Provides for flexibility and tailoring:

- Adjust to current organization
- Emphasize areas of interest
- Supports informal assessment construction

SECAM Modification

Three basic areas of the SECAM:

I. Management Processes

II. Organization Processes

III. Systems Engineering Processes

Modification of the SECAM basic areas:

Management Processes – **minor** modification

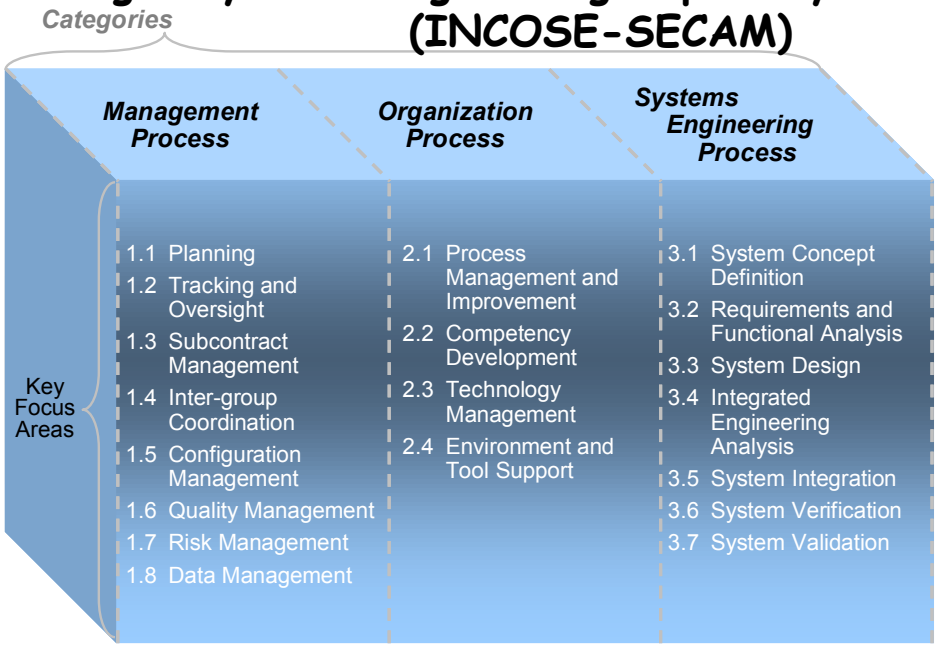
Organization Processes – **minor** modification

Systems Engineering Processes – delete, then add new section

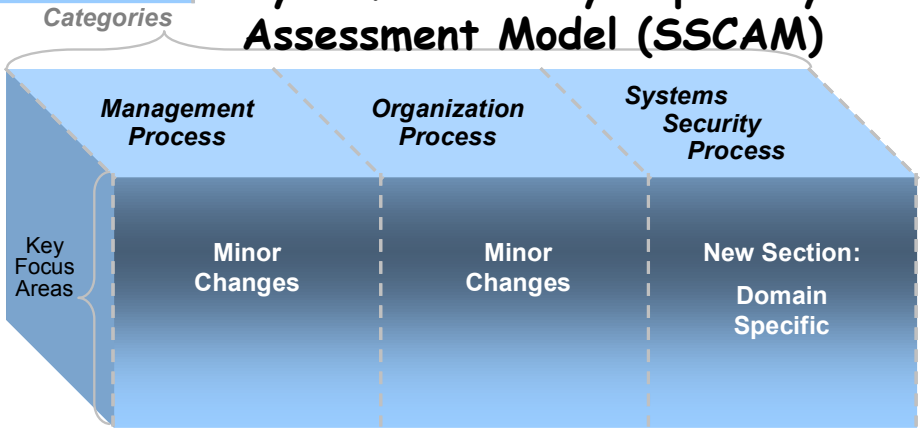
- Add new section of global security concerns
- Develop new domain specific sections as "plug-ins"

Relationship Between SECAM and SSCAM

Existing: Systems Engineering Capability Assessment Model (INCOSE-SECAM)

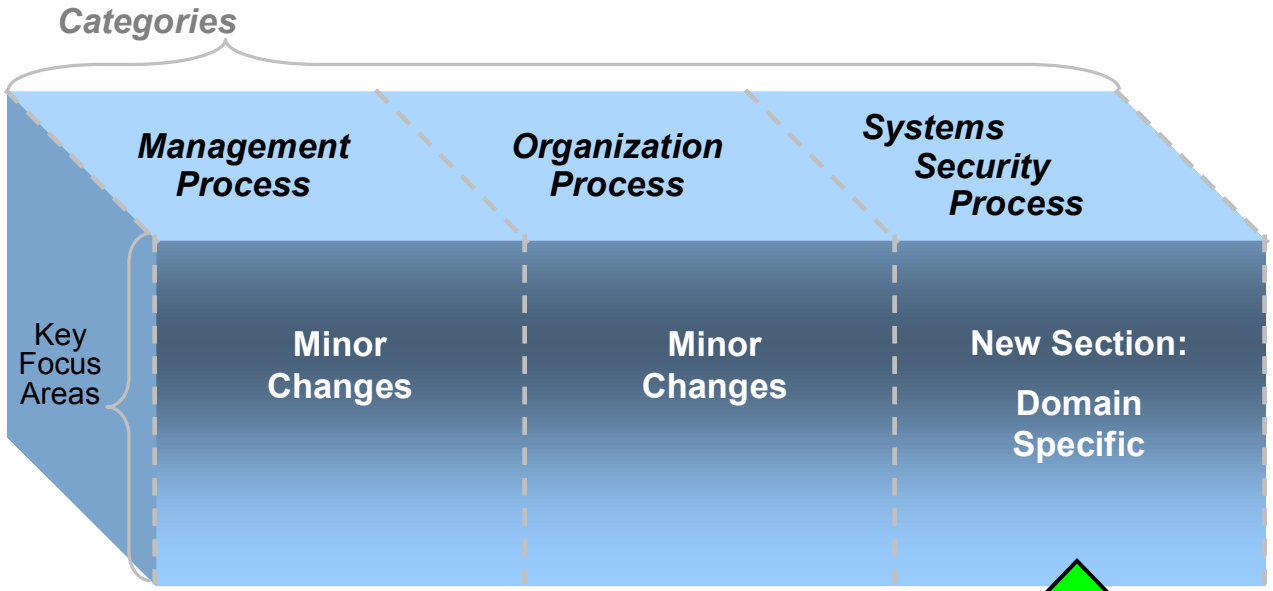


Proposed: Systems Security Capability Assessment Model (SSCAM)

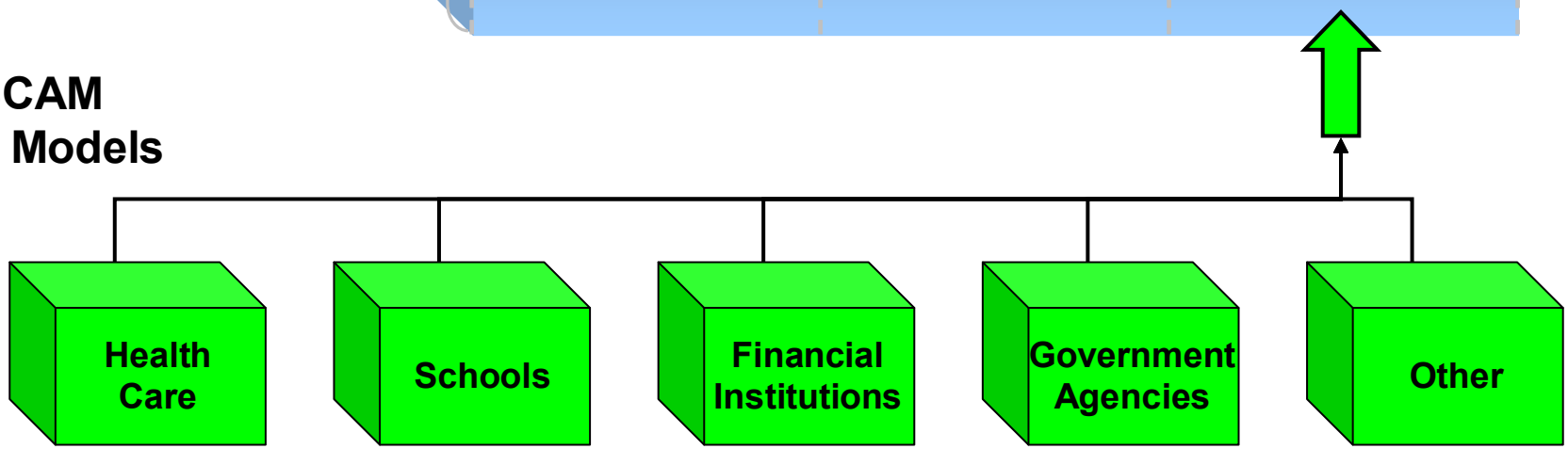


Relationship Between Global Level and Local Level

SSCAM Global Model



SSCAM Local Models



SSCAM Purpose, Structure and Organizational Support

The SSCAM supports the assessment of an organizations security operations capability in a dynamic threat context

Three application areas of the SSCAM:

1. Domain Specific Management Processes
2. Domain Specific Organization Processes
3. Domain Specific Systems Security Processes

Two SSCAM model types:

1. SSCAM Global Model
2. SSCAM Local Model

Models supported by a set of industry, government and academic advisory boards

SSCAM Quick Look Concepts

The SSCAM Quick Look Model focuses on the fundamental aspects needed to effectively perform secure operations.

Screening model used to quickly develop the structured information required to determine if a more robust, in-depth security assessment would be of value.

Focus on three key groups of activities:

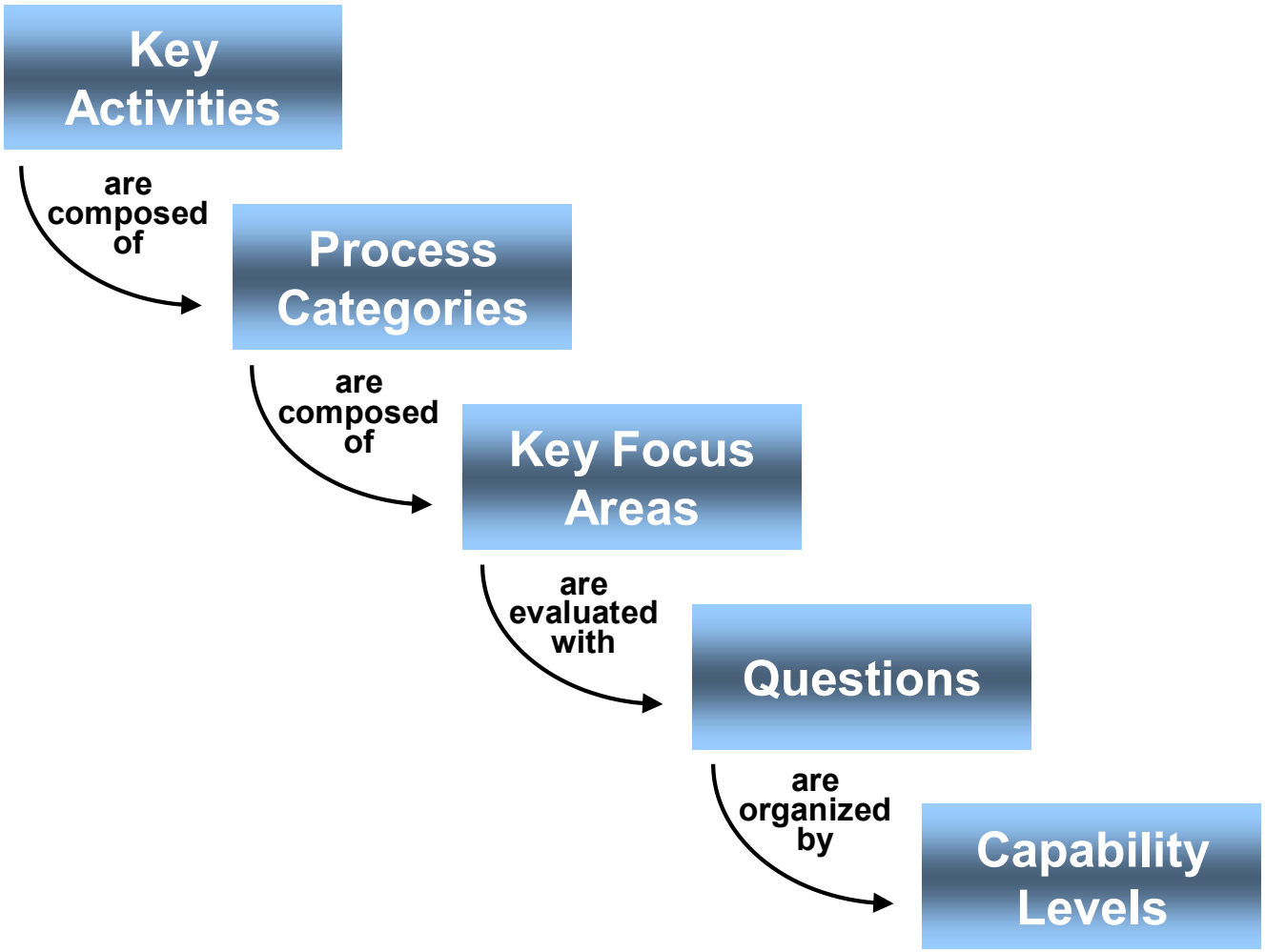
- Key **contextual** activities
- Key **organizational** activities
- Key **development** activities

SSCAM Quick Look Structure

The SSCAM Quick Look Model structure is a hierarchy of related concepts and facts

- Key Activities
- Process Categories
- Key Focus Areas
- Questions
- Capability Levels

SSCAM Quick Look Structure



SSCAM Quick Look Assessment Method

SSCAM Quick Look Assessment Goals:

Goal One - Measure an organizations system security awareness and capability.

Goal Two – Identify and document system security problem areas and concerns

Goal Three – Provide a baseline analysis that is the foundation for growth in system security capability.

SSCAM Quick Look Assessment Components

SSCAM QL Assessment Overview

SSCAM QL Assessment Method Activities

SSCAM QL On-Site Planning Templates

SSCAM QL Questionnaire

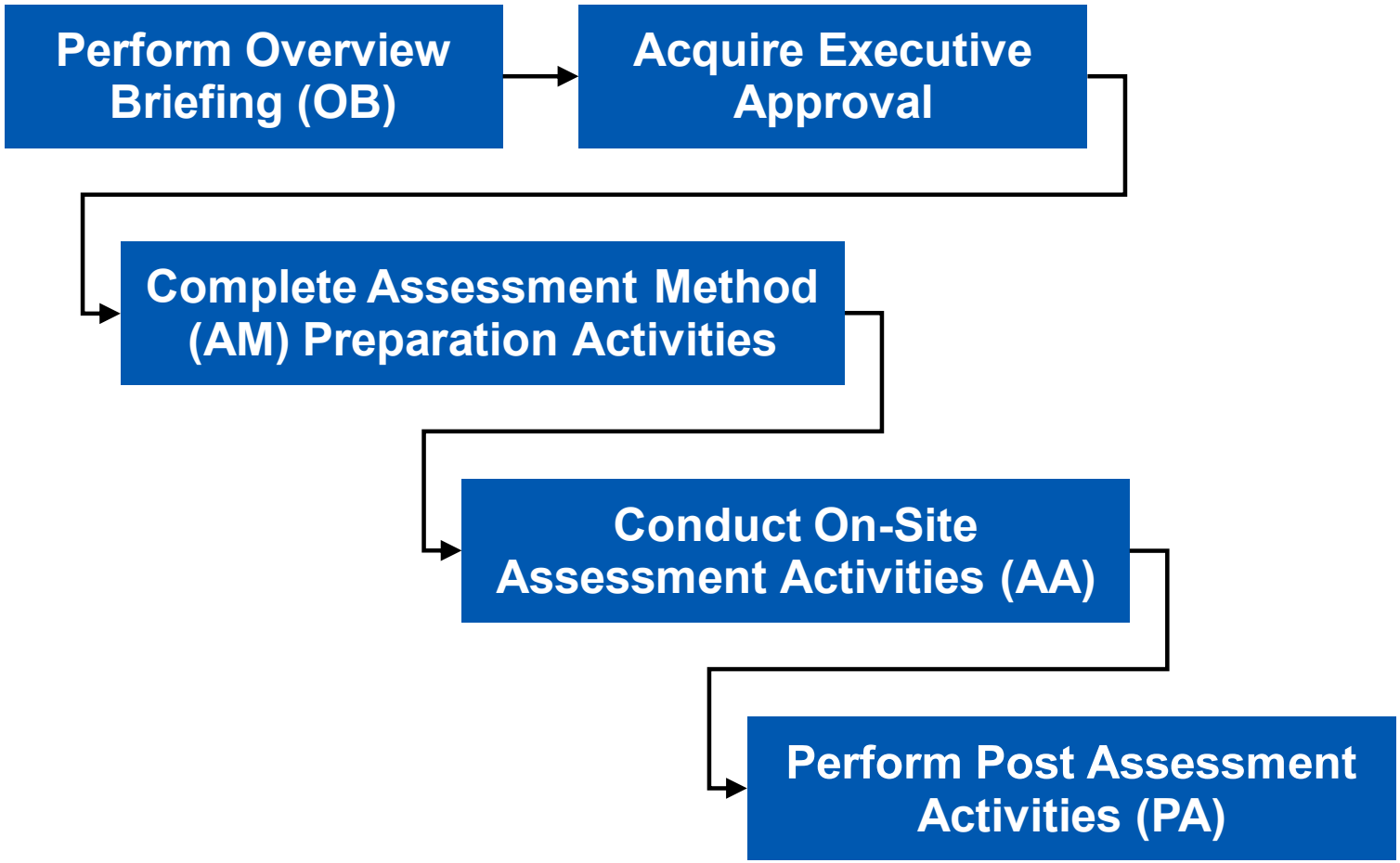
Exploratory Questions

Heuristic Scoring Method and Template

Presentation Templates

Assessment Survey

Security Quick Look Assessment Steps



Overview Briefing Contents

Assessment Principles and Purpose

Assessment Conduct Guidelines

Assessment Outcomes and Products

Assessment Schedule Executive Level Approval

Assessment Activity Executive Level Approval

Clear Communication of the Executive Level Decision to the Organizational Elements

Assessment Method - Preparation Activities

1. Form Planning Team
2. Characterize the Organization to be Assessed
3. Develop an Organizational Assessment Strategy
4. Develop Assessment Draft Action Plan
5. Provide Assessment Orientation
6. Tabulate a Practice Questionnaire Data Set

On-Site SQLA Activities (1 of 2)

1. Conduct Assessment Opening Meeting
2. Prepare Assessment Team Members
3. Conduct Individual Interviews
4. Conduct Group Discussions
5. Summarize Issues and Outcomes
6. Review Issues With Individual Participants

On-Site SQLA Activities (2 of 2)

7. Develop Assessment Findings
8. Present Draft Findings to the Individuals and Group Participants
9. Review Comments
10. Review Findings
11. Management Final Findings Presentation
12. Develop and Summarize Lessons Learned

Post Assessment Activities

Document the Assessment Results

Draft Process Improvement Action Plan

Conduct Complete System Security Capability Assessment (if necessary)

Seek Executive Approval to Implement Action Plan

Implement System Security Action Plan

Assessment Questions

The SSCAM QL questions address the three key areas at a very high level.

- Does the organization understand the operational security context and obligations?
- Does the organization have a clear operational security control and accountability established?
- Do adequate security operational and developmental processes exist, and are they enforced?

Summary and Conclusions

- System security is becoming much more important.
- A relatively high number (70%) of software development groups do not use a secure system development life-cycle.
- Security-related legal risks are becoming larger and more costly.
- The SQL Method was developed from the INCOSE SECAM to support the structured evaluation of an organizations' security capability.
- The University of Washington's Center for Information Assurance and Cybersecurity (UW-CIAC) invites participation in further development activities.

UW-CIAC Contact Information

Dr. Barbara Endicott-Popovsky, Director
Center for Information Assurance and Cybersecurity
University of Washington
4311 11th Ave NE Suite 40
Box 354985
Seattle, Washington 98105
endicott@u.washington.edu
206-284-6123