Booz | Allen | Hamilton

EWA
. . . where concepts become realities.

HARRIS®

LOCKHEED MARTIN

ISO/IEC 21827
Systems Security Engineering Capability Maturity Model (SSE-CMM)

A Process Driven
Framework for Assurance

Booz | Allen | Hamilton

EWA
. . . where concepts become realities.

HARRIS

LOCKHEED MARTIN

Information Systems Security Engineering Association (ISSEA)

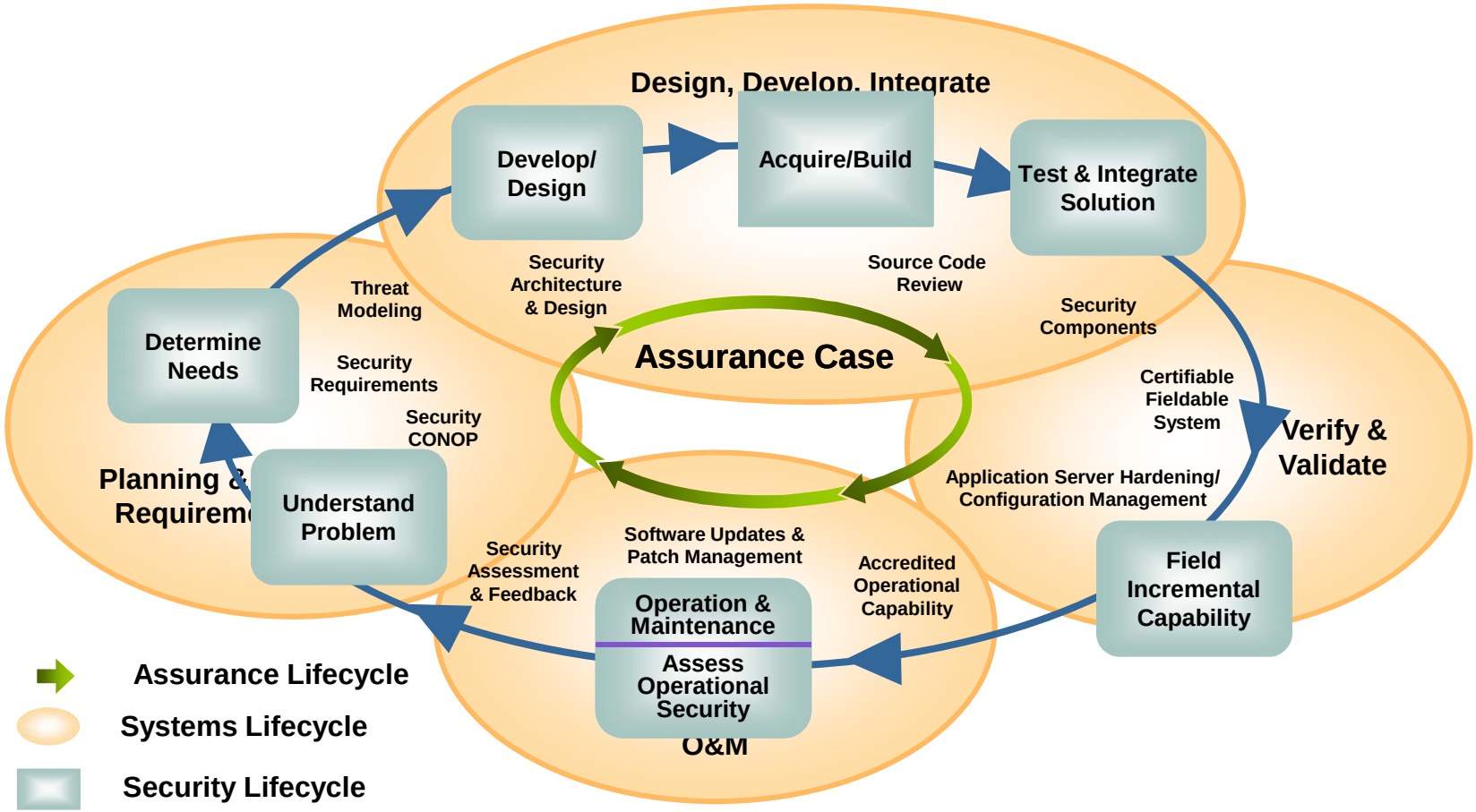
- ISSEA is an industry organization that …
  - promotes and enhances the Systems Security Engineering –Capability Maturity Model (SSE-CMM / ISO 21827) and derivatives
    - Transportation Sector derivative (published)
    - Medical Sector (Under consideration)
    - Financial Sector (Under consideration)
  - dedicated to the advancement of systems security engineering as a defined and measurable discipline
  - running an ongoing effort to identify opportunities to collaborate with other initiatives for aligning with SSE CMM to promote mature security capability among system and software developers

Assurance Road Map

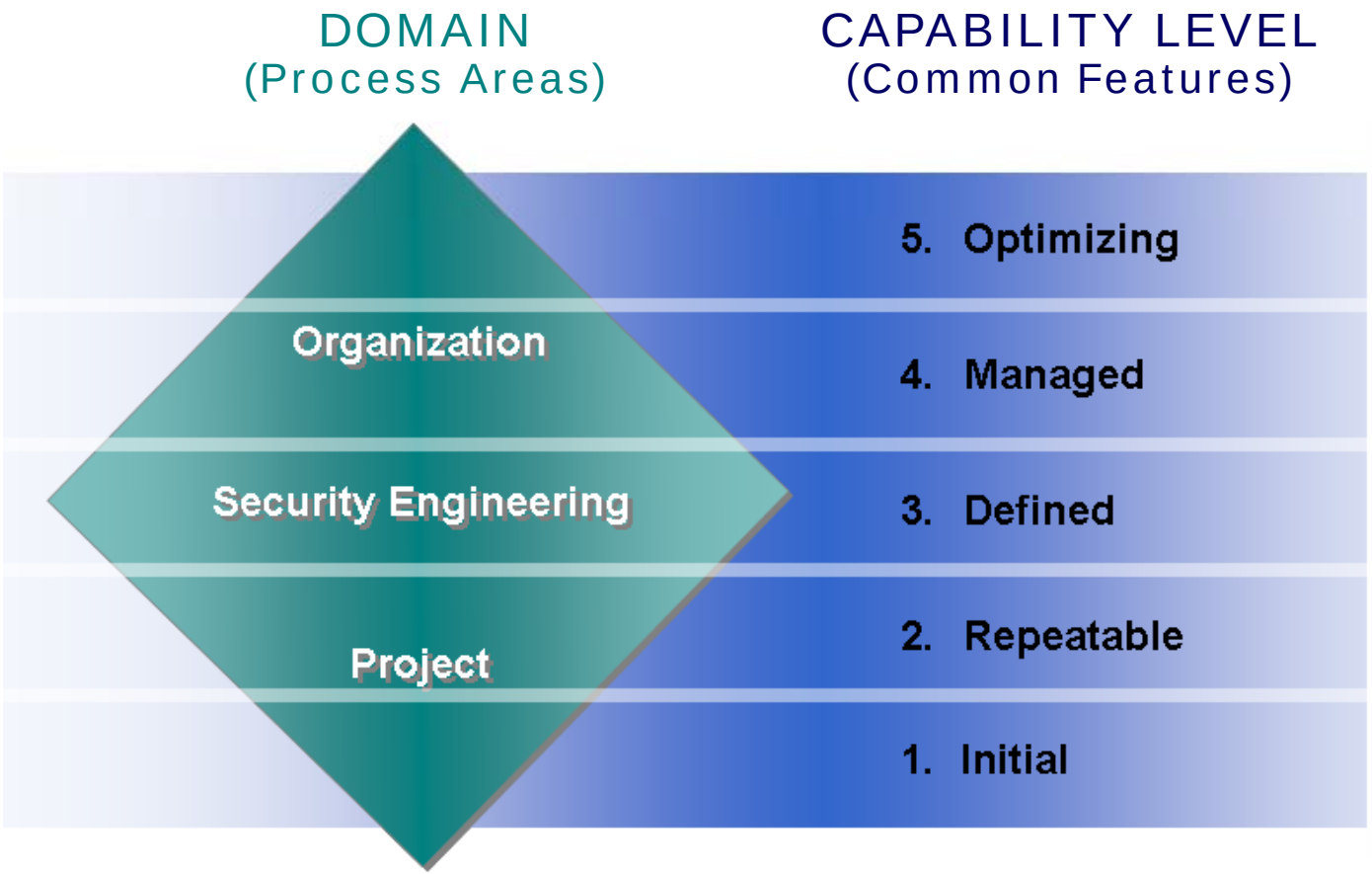
- The ISO/IEC 21827 can help…
  - Identify Security Goals
  - Assess Security Posture
  - Support Security Life Cycle
    - Identify Risks
    - Establish Security Requirements
    - Implement Controls
    - Determine Effectiveness

ISSEA Booz | Allen | Hamilton EWA . . . where concepts become realities. HARRIS LOCKHEED MARTIN

ISO/IEC 21827 is a content-independent standard, which facilitates implementation of a good process for ANY set of security practices



ISO/IEC 21827
Model Dimensions



Booz | Allen | Hamilton

EWA
. . . where concepts become realities.

HARRIS

LOCKHEED MARTIN

Model Process Areas

Security Engineering Process Areas	# of Base Practices
Administer Security Controls	4
Assess Impact	6
Assess Security Risk	6
Assess Threat	6
Assess Vulnerability	5
Build Assurance Argument	5
Coordinate Security	4
Monitor Security Posture	7
Provide Security Input	6
Specify Security Needs	7
Verify and Validate Security	5

Project and Organizational Process Areas	# of Base Practices
Ensure Quality	8
Manage Configuration	5
Manage Project Risk	6
Monitor and Control Technical Effort	6
Plan Technical Effort	10
Define Organization's Security Engineering Process	4
Improve Organization's Security Engineering Process	4
Manage Product Line Evolution	5
Manage Systems Engineering Support Environment	7
Provide Ongoing Skills and Knowledge	8
Coordinate with Suppliers	5

ISO/IEC 21827 Appraisal

- Evidence based appraisal method
  - Provides “As Is” picture
  - Tailored to the organization
  - Supports business/ mission objectives
  - Identifies areas for Improvement

Measuring Assurance

- ISO/IEC 21827 compliant processes can be measured and managed to …
  - Tie security practice performance to business and security goals
  - Quantify compliance with standards
  - Measure effectiveness and efficiency of security implementation
  - Identify data used for measurement
- Measures allow us to…
  - Repeat measurement and provide relevant performance trends over time
  - Identify opportunities for corrective actions and formulate action plans
  - Support security improvement and budget recommendations
  - Produce evidence that substantiates assurance cases

Summary

- ISO/IEC 21827 provides a roadmap for establishing and maturing security practices
  - Process Areas identify a comprehensive set of base (security) practices
  - Capability Levels define maturity
- ISO/IEC 21827 (SSE-CMM) appraisals
  - use process implementation evidence
  - gain insight into maturity and institutionalization of security processes and practices
- Process implementation evidence
  - results from use of the SSE-CMM
  - creates tangible data that can be leveraged in an assurance case

Contact Information

- Joyce F. Richardson
  (301)313-3927
  joyce.f.richardson@lmco.com
- Nadya Bartol
  703-377-1252
  bartol_nadya@bah.com
- Michele Moss
  703-377-1254
  moss_michele@bah.com

- www.issea.org
- www.sse-cmm.org

International Systems Security Engineering Association
13873 Park Center Road, Suite 200
Herndon, VA 20171

REFERENCES:
"*Measuring Capability Based Assurance" – NETSEC JUNE '04 Proceedings (Nadya Bartol & Joyce Richardson)*
"ISO/IEC 21827" – version 2.0