

ISO 21827 System Security Engineering Capability Maturity Model

Presented By John W. Lindquist
Founding Member of the HIPAA Alliance, LLC and President and CEO
EWA Information & Infrastructure Technologies, Inc.
13873 Park Center Rd., Ste. 200, Herndon VA 20171
703 478 7600

6th Annual HIPAA Summit
Session: 5.06 On-Going HIPAA Compliance: Securing Tracked Data - March 28, 2003

HIPAA·CAAT

IIT An EWA Company



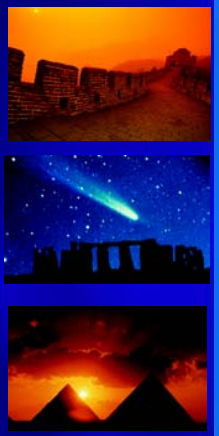
Problem

How does management establish and track an information security program when:

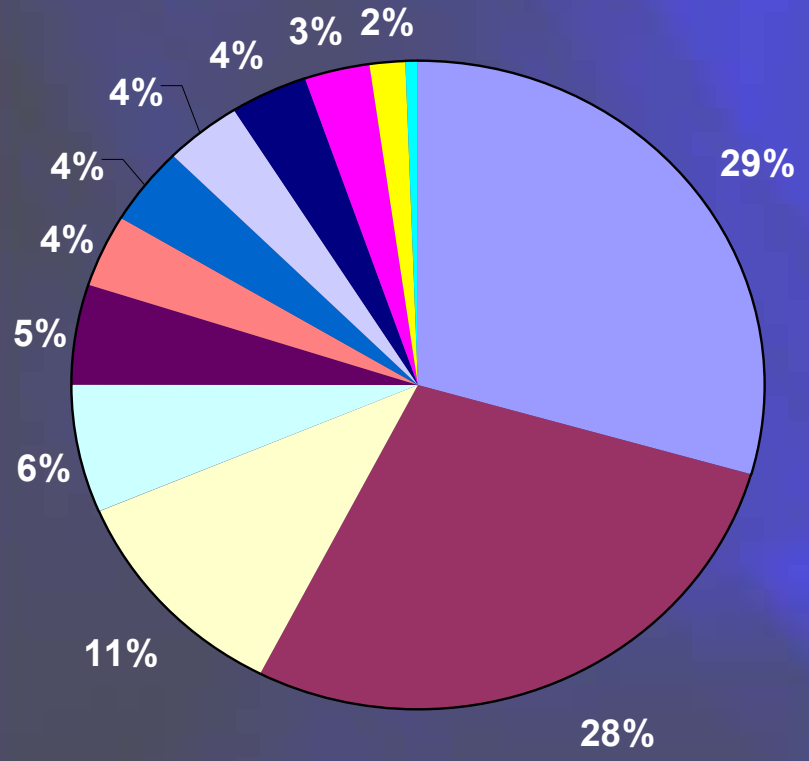
- Risks are real
- Risks are nearly infinite
- The information environment is highly dynamic
- Resources are finite

HIPAA·CAAT

IIT An EWA Company



The Need to Protect



Information assets against damage and unauthorized disclosure is critical to your organization.

HIPAA·CAAT

IIT An EWA Company



Information Assurance

Solutions Must Address:

- People
- Process
- Technology

Technology alone won't make you safe.

"Get rid of the techno-babble. This is a management problem."

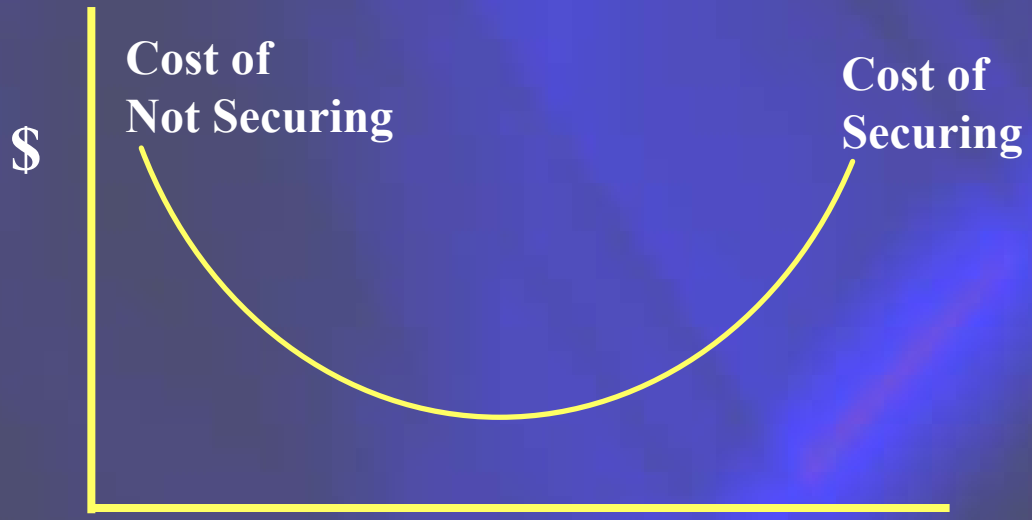
Steve Katz, CISO, Citibank

HIPAA·CAAT

IIT An EWA Company



Process Maturity and the Risk Management Cost Continuum



Security Aversion (Ostrich) — **Risk Management Decisions** (Acceptance, Mitigation, Transference, Avoidance) — **Risk Aversion** (Paranoia)

Level 0 — **SSE-CMM Process Maturity** (Focused investment in IT Security) — **Level 5**

HIPAA·CAAT

IIT An EWA Company



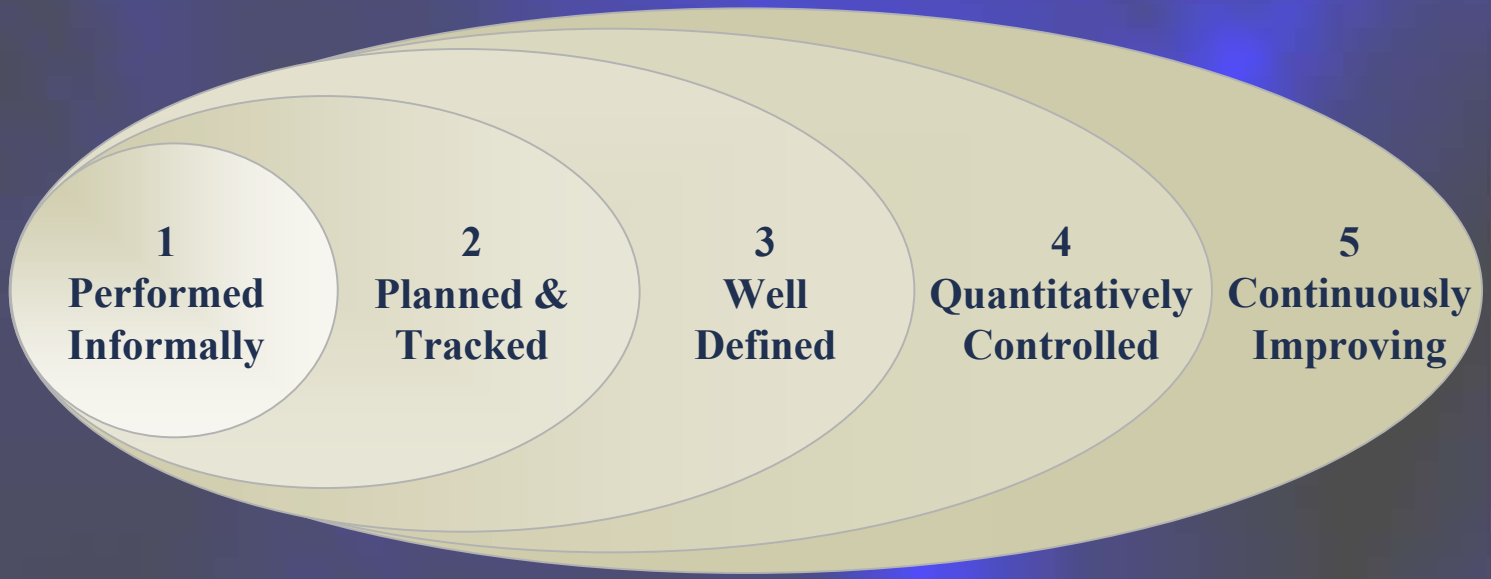
SYSTEM SECURITY ENGINEERING CAPABILITY MATURITY MODEL

- SSE - CMM is both a Model and a Process
- A Community-owned Model (50 companies / agencies led by the US National Security Agency (NSA) and Canadian Communications Security Establishment (CSE))
- Model Presents Security Engineering as a Defined, Mature and Measurable Discipline
- Model and Appraisal Method Enable:
  - Capability-based assurance i.e.. Security/trustworthiness inferred from the maturity of processes
  - Focused investment in security engineering tools, training, process definition, management practices and improvements based on risk assessment and available resources
  - Qualifying vendors, suppliers, and organizations connecting to a system

HIPAA·CAAT

IIT An EWA Company

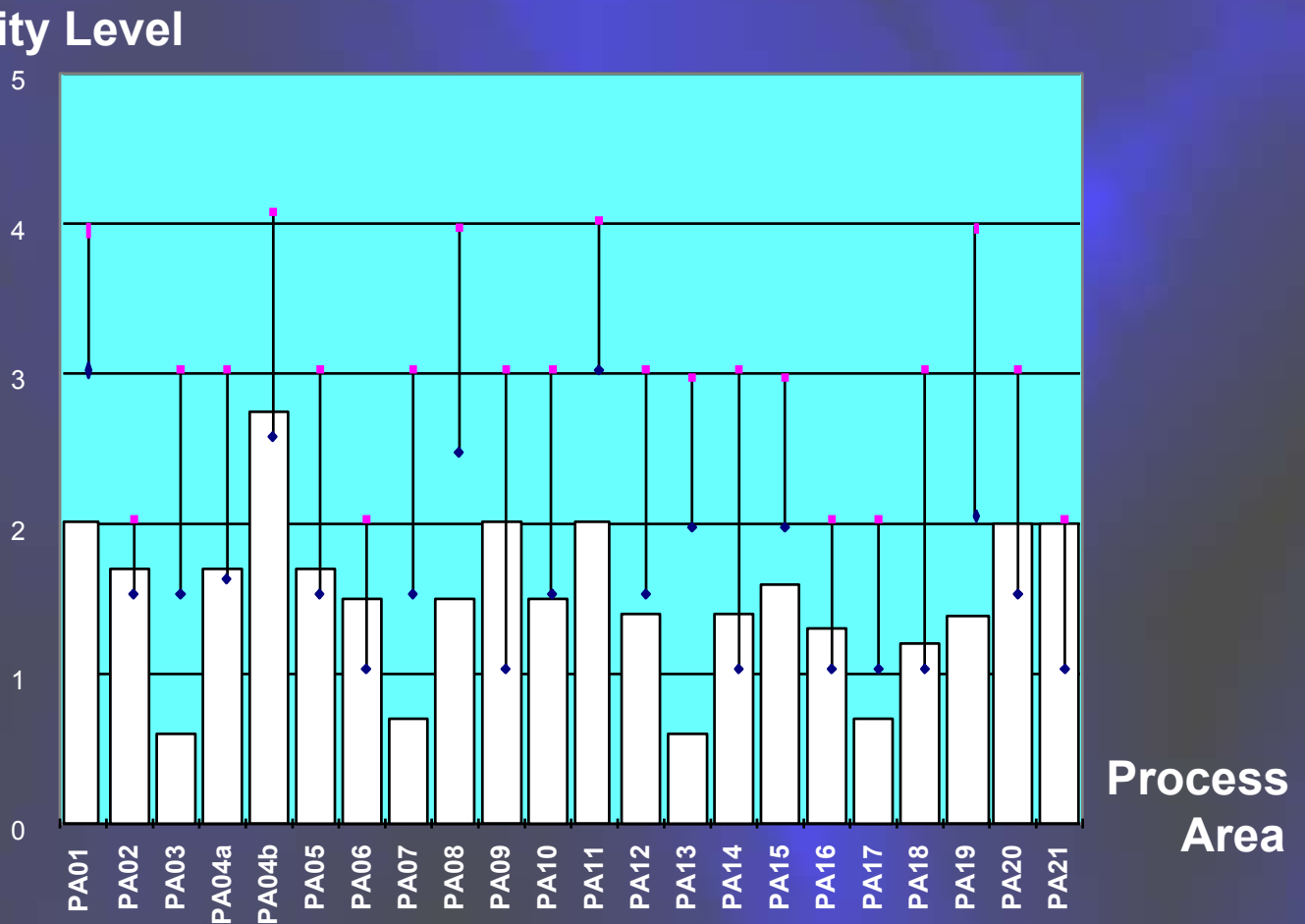
CAPABILITY LEVELS



HIPAA·CAAT

IIT
An EWA Company

Baseline, Minimum & Target Profile



HIPAA·CAAT

IIT An EWA Company



HIPAA·CAAT

IIT An EWA Company

System Security Process Areas

PA 01 Specify Security Needs

PA 02 Provide Security Input

PA 03 Verify and Validate Security

PA 04a Threat Assessment

PA 04b Impact Assessment

PA 05 Assess Security Risk

PA 06 Build Assurance Argument

PA 07 Monitor System Security Posture

PA 08 Administer Security Controls

PA 09 Coordinate Security

PA 10 Vulnerability Assessment

PA 11 Ensure Quality

PA 12 Manage Configurations

PA 13 Manage Program Risk

PA 14 Monitor and Control Technical Effort

PA 15 Plan Technical Effort

PA 16 Define Organization's Security Engineering Process

PA 17 Improve Organization's Security Engineering Processes

PA 18 Manage Security Product Line Evolution

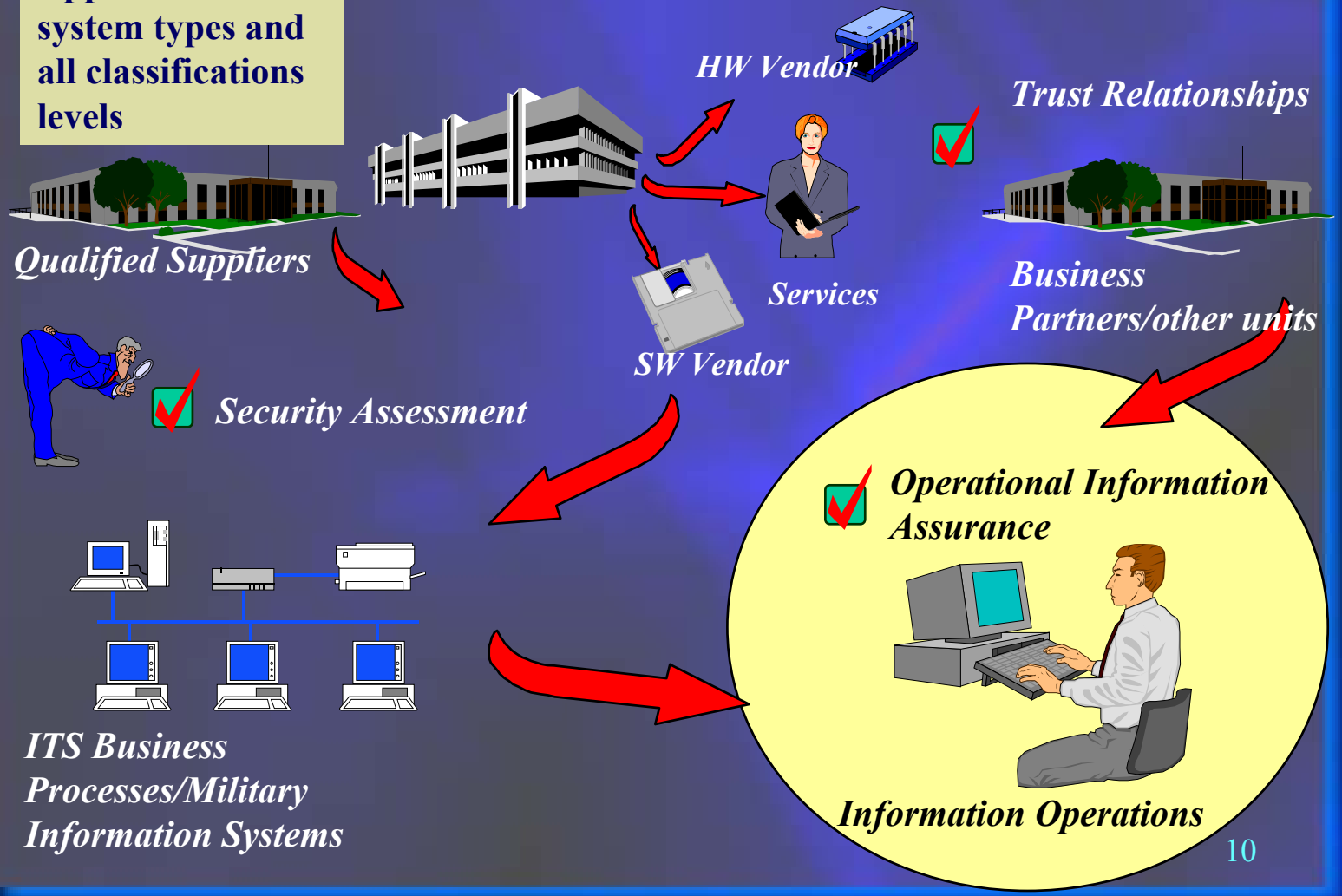
PA 19 Manage Security Engineering Support Environment

PA 20 Provide Ongoing Skills and Knowledge

PA 21 Coordinate With Suppliers

SSE-CMM Usage Scenarios

Applies to all system types and all classifications levels





Summary

- Can't Protect Everything All The Time
- The Dynamic Environment Requires a Flexible Response
- Effective Information Assurance Must Address People, Process and Technology
- Information Assurance is Risk Management not Risk Avoidance (There is No Silver Bullet)
- The SSE-CMM is an IA Tool Developed in Consideration the Above

HIPAA·CAAT

IIT An EWA Company