

System Assurance Evaluation

Han, Jongwoo
System Assurance
Institute &
The Maxwell School

Why Signature Project?

- First MT
- Four colleges' roles in SAI & SAI
- Assurance as an essential part of E-government
- High visibility
- Fund raising

Why Evaluation?

- GPRA in 1993
- OMB (PART)
- OMB Circular A-130, Appendix III
"Security of Federal Automated
Information Resources"

Why Evaluation?

- 9/11 & Cyber Security Act
- GISRA (Government Information Security Reform Act)
- Presidential Decision Directive 63

Agencies

- OMB
- Congress GAO
- For CIO Council
- NIST

Overall Federal Evaluation Structure

- GPRA
- President's Management Agenda
- Executive Branch Management Scorecard
- PART
- Common Performance Measures

Government Evaluation Projects

- GPP by The Maxwell's Campbell Institute
- FPP by

GPP

	IT Mana.	Finan M	HR	Capital M	M f Results
Architect.	25%				
M Support	25%				
Planning	15%				
Citizen P.	15%				
C/B Analysis	10%				
Procure.	5%				
Training	5%				

Lessons

- Resistance from Bureaucracy
- Partnership & collective learning
- "Help" and DO NOT "Don't Help"
- Not Relative Scoring but Customized Consulting, Advice
- Graduate Student Internship for effective communications

IT Investment Management Process (GAO)

	Select	Control	Evaluation
Process	Validity C/B, portfolio	Program monitor, HR, Records, Feedbacks	Post-Eval. Feedbacks
Data			
Decisions			

NIST, Information Technology Laboratory (ITL)

- National Institute of Standards and Technology: <http://csrc.nist.gov/>
- Special Publication 800-26, "Self-Assessment Guide for IT Systems"
- Cryptographic Standards and Application
- Cryptographic Module Validation (CMV) Program <http://csrc.nist.gov/cryptval/>
- Security Testing

What is IT Security Assurance

- “the degree of confidence one has that the managerial, technical and operational security measure work as intended to protect the system and the information it processes” (NIST)

Trustworthiness

- Correctness: proper outputs by each input
- Availability: continuation of operation
- Security: resistance against certain attacks
(Secrecy, confidentiality, integrity, availability)
- Privacy
- Safety
- Survivability

SSE-CMM

- Systems Security Engineering-Capability Maturity Model
- <http://sse-cmm.org/>

Evaluation Structure

- Who: Managers
- What: Policy, system data, reports, analysis

Evaluation Process

- Data Collection: Gathering and Entering system data
- Reporting: Creating aggregate data
- Analysis: Understanding, Evaluating, Making Judgements
- Manager, Collector, Reporter, SME (Subject Matter Expert:SAI)

NIST Evaluation

- Develop Annual Performance & Improvement Measure
- Confidentiality, Integrity, Availability by five levels
- Cost-effectiveness

5 Levels

- Level 1: Policy
- Level 2: Procedures
- Level 3: Implemented
- Level 4: Tested
- Level 5: Integrated

Category of Criticality

	Confidentiality	Integrity	Availability
Low			
Medium			
High			

NIST System Questionnaire

- Management Controls
- Operational Controls
- Technical Controls

Management Controls

- Risk Management
- Review of Security Controls
- Life Cycle
- Authorize Processing (Certification & Accreditation)
- System Security Plan

Operational Controls

- Personnel Security
- Physical and Environmental Protection
- Production, Input/Output Controls
- Contingency Planning
- Hardware and System Software Maintenance

Operational Controls continued

- Data Integrity
- Documentation
- Security Awareness, Training, and Education
- Incident Response Capability

Technical Controls

- Identification and Authentication
- Logical Access Controls
- Audit Trails

Legislations

- The Government Information Security Reform Act of 2000
- The Cyber Security Enhancement Act of 2002 (HR. 3482)
- Cyber Security Research and Development Act of 2002

What makes SAI Signature project different?

- Local & State governments: Law-enforcement agencies, EOC
- Customization: Prescriptions, Risk Analysis
- Unique environment of Local Governments Information System
- Enticing Voluntary participation (Invitation to Local CIOs to Spring Conference)
- Graduate Internship-- NSA designation

What This Means

- Form a committee with each agency
- Link System Evaluation with Budget
- Assisting System Security Investments
- Apply the concept of E-Governance Grid to local settings

Key to Success

- Information mind of leaders
- Partnership
- Learning rather than teaching

Plan

- Government relations
- Basic Survey: Preliminary research on research objects
- Case Customization
- Major Directions: Confidentiality, Integrity, Availability