U.S. DEPARTMENT OF ENERGY

New Orleans, Louisiana
Monday, March 2, 2009 – Friday, March 6, 2009

Information Management Conference

Raising the Bar…Seeking Innovative Solutions for Tomorrow's Challenges

INFORMATION Management Conference

Lessons Learned from Federal Agencies using the NIST PRISMA Model for Measuring Security Maturity

By

John M. Abeles, System 1, Inc.
(301)792-4581 – jabeles@syst1.com

Questions to be answered today

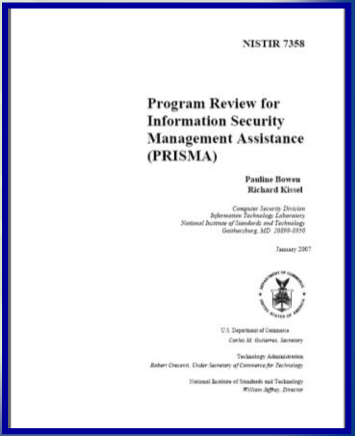
- What is PRISMA?
- How does it work?
- What has been observed and can be learned from other Federal agencies where PRISMA has been used?
- What has been managements' reaction to PRISMA results?

What PRISMA is

- Program Review for Information Security Management Assistance is PRISMA
  - Published by NIST in 2007
  - Security Maturity Model with an corresponding database

- Used to establish a baseline score card of security maturity and for continuous monitoring
  - At the Department level and at the program/bureau level
  - Promotes transparency and focuses accountability

- Briefed to Congress and recommended by CSIA in 2008



NISTIR 7358

Program Review for Information Security Management Assistance (PRISMA)

Pauline Bowen
Richard Kissel

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

January 2007

U.S. Department of Commerce
Carlos M. Gutierrez, Secretary

Technology Administration
Robert Cresanti, Under Secretary of Commerce for Technology

National Institute of Standards and Technology
William Jeffrey, Director

How PRISMA works

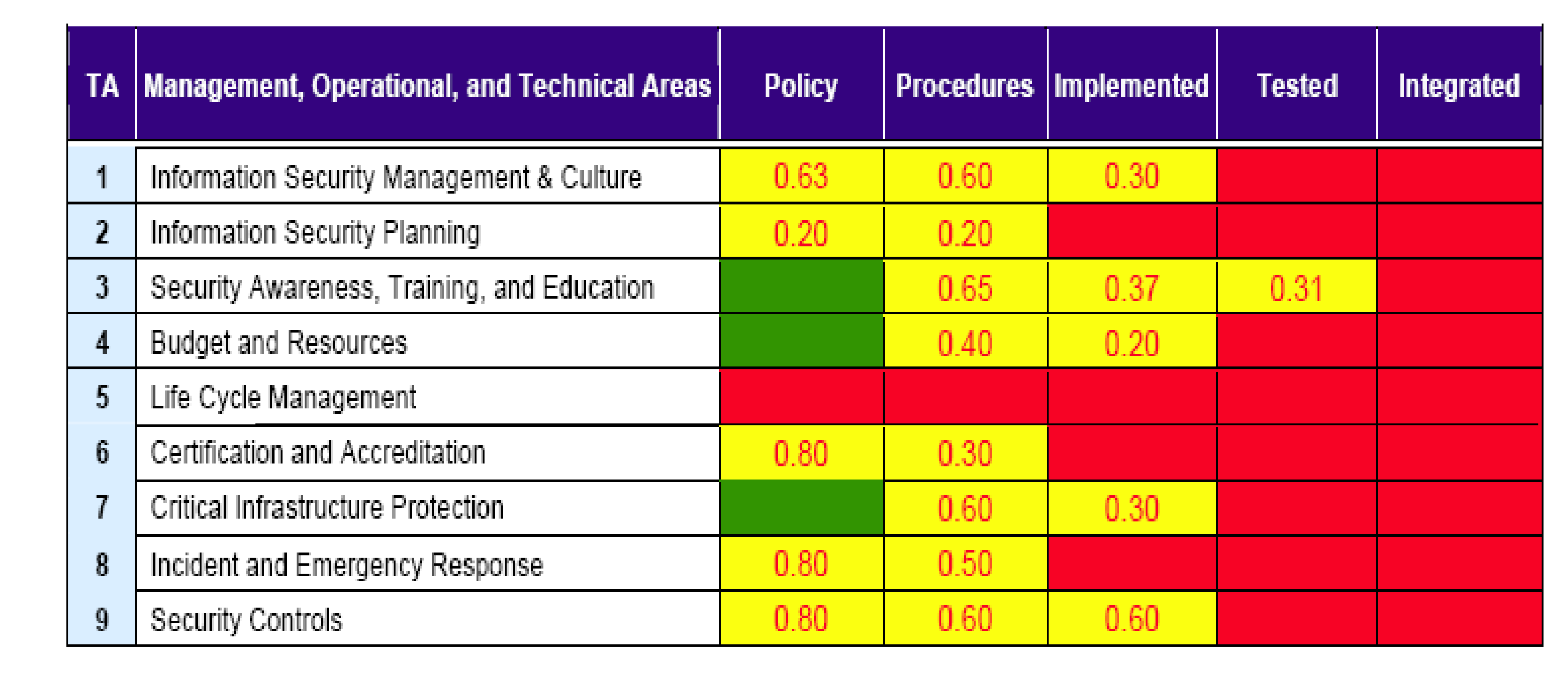
- PRISMA Assessment is conducted in two parts

- Documentation Review
  - Are the policies and procedures documented, accurate, and readily available?
  - Is security part of integrating programs (SDLC, PM, CPIC, EA) and mission delivery?

- Interview Review
  - Are security policies and procedures improved as part of the security program life cycle?
  - Are security policies and procedures implemented (followed by the site personnel, integrated into normal operations)?

PRISMA
2 parts common sense
1 part intuition
1 part knowledge
1 part experience

Sample PRISMA Scorecard



TA	Management, Operational, and Technical Areas	Policy	Procedures	Implemented	Tested	Integrated
1	Information Security Management & Culture	0.63	0.60	0.30	🟥	🟥
2	Information Security Planning	0.20	0.20	🟥	🟥	🟥
3	Security Awareness, Training, and Education	🟩	0.65	0.37	0.31	🟥
4	Budget and Resources	🟩	0.40	0.20	🟥	🟥
5	Life Cycle Management	🟥	🟥	🟥	🟥	🟥
6	Certification and Accreditation	0.80	0.30	🟥	🟥	🟥
7	Critical Infrastructure Protection	🟩	0.60	0.30	🟥	🟥
8	Incident and Emergency Response	0.80	0.50	🟥	🟥	🟥
9	Security Controls	0.80	0.60	0.60	🟥	🟥

Legend: Green = fully compliant
Yellow = partially compliant
Red = non compliant

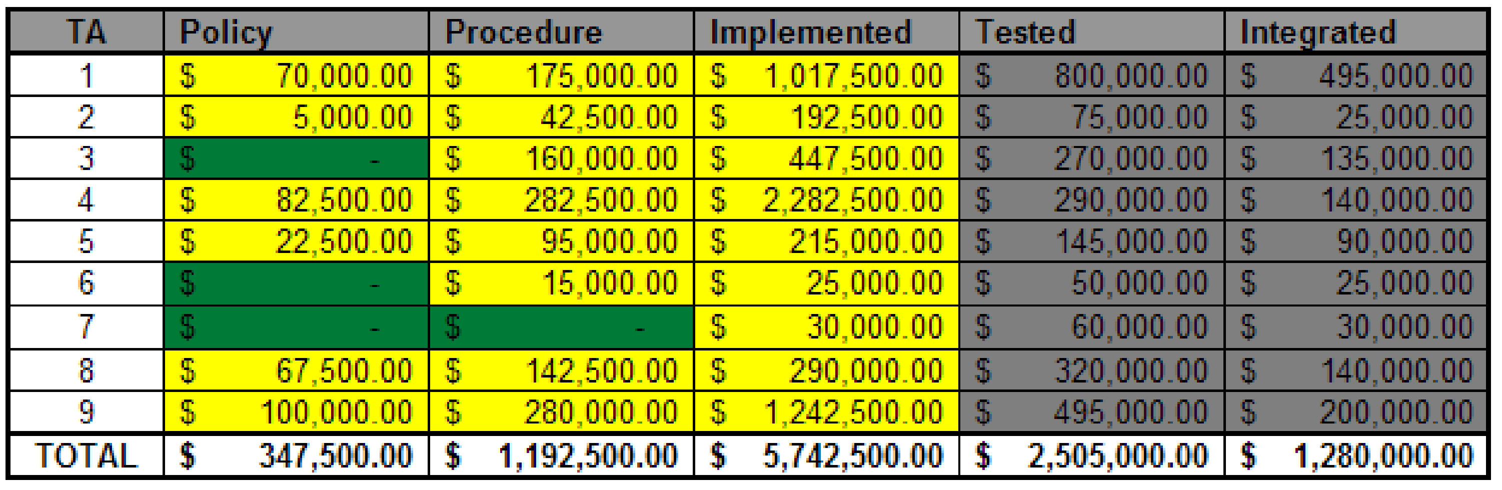
Scorecards are also generated for subtopics in each of the 9 topic areas.

PRISMA Report/Output

- **Program Status**
  - – Maturity Scorecards in 9 topic areas, 30 subtopic areas
    - This can be done for a Department and at a Program or Site level
    - Score can be aggregated to Department overall scorecard
- **Evaluation of each topic area**
  - – Observations
  - – Issues
  - – Recommendations
- **Recommended Action Plan**
  - – Issues and recommendations
  - – Timeframe to implement
  - – Resource Impact
- **Database**
  - – Baseline that can be periodically updated to track security improvement

Financial Impact – Value Added

- **Bottom-up analysis**
  - Cost to achieve each subtopic criteria aggregated for topic area total cost

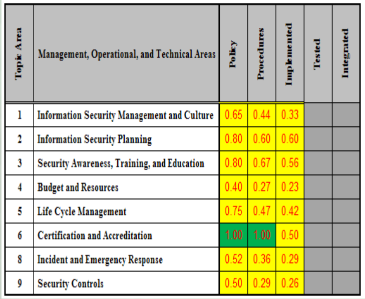


TA	Policy	Procedure	Implemented	Tested	Integrated
1	$ 70,000.00	$ 175,000.00	$ 1,017,500.00	$ 800,000.00	$ 495,000.00
2	$ 5,000.00	$ 42,500.00	$ 192,500.00	$ 75,000.00	$ 25,000.00
3	$ -	$ 160,000.00	$ 447,500.00	$ 270,000.00	$ 135,000.00
4	$ 82,500.00	$ 282,500.00	$ 2,282,500.00	$ 290,000.00	$ 140,000.00
5	$ 22,500.00	$ 95,000.00	$ 215,000.00	$ 145,000.00	$ 90,000.00
6	$ -	$ 15,000.00	$ 25,000.00	$ 50,000.00	$ 25,000.00
7	$ -	$ -	$ 30,000.00	$ 60,000.00	$ 30,000.00
8	$ 67,500.00	$ 142,500.00	$ 290,000.00	$ 320,000.00	$ 140,000.00
9	$ 100,000.00	$ 280,000.00	$ 1,242,500.00	$ 495,000.00	$ 200,000.00
TOTAL	$ 347,500.00	$ 1,192,500.00	$ 5,742,500.00	$ 2,505,000.00	$ 1,280,000.00

- **Top Down Method**
  - Top-down approach estimating cost for implementing recommendations from PRISMA report
  - Organization specific factors considered

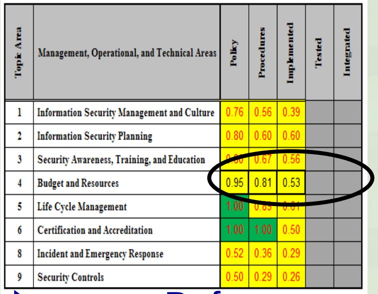
Roadmap to improvement

- **Benefit Projection**
  - PRISMA maturity level evaluation based on recommended action plan and actionable steps within a specified timeframe
  - Performance measurements to define return on investment, justify business cases, and evaluate effectiveness
  - Shows progressive improvement and defines benefits costs, and implementation schedule to senior management



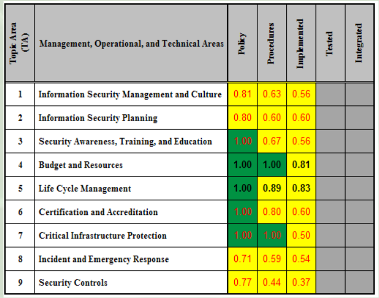
Topic Area	Management, Operational, and Technical Areas	Policy	Procedures	Implemented	Tested	Integrated
1	Information Security Management and Culture	0.65	0.44	0.33		
2	Information Security Planning	0.80	0.60	0.60		
3	Security Awareness, Training, and Education	0.80	0.67	0.56		
4	Budget and Resources	0.40	0.27	0.23		
5	Life Cycle Management	0.75	0.47	0.42		
6	Certification and Accreditation	1.00	1.00	0.50		
8	Incident and Emergency Response	0.52	0.36	0.29		
9	Security Controls	0.50	0.29	0.26		

Implement a group of recommendations



Topic Area	Management, Operational, and Technical Areas	Policy	Procedures	Implemented	Tested	Integrated
1	Information Security Management and Culture	0.76	0.56	0.39		
2	Information Security Planning	0.80	0.60	0.60		
3	Security Awareness, Training, and Education	0.80	0.67	0.56		
4	Budget and Resources	0.95	0.81	0.53		
5	Life Cycle Management	1.00	0.89	0.81		
6	Certification and Accreditation	1.00	1.00	0.50		
8	Incident and Emergency Response	0.52	0.36	0.29		
9	Security Controls	0.50	0.29	0.26		

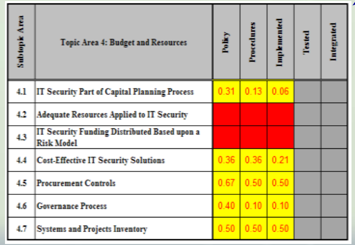
Implement a group of recommendations



Topic Area (TA)	Management, Operational, and Technical Areas	Policy	Procedures	Implemented	Tested	Integrated
1	Information Security Management and Culture	0.81	0.63	0.56		
2	Information Security Planning	0.80	0.60	0.60		
3	Security Awareness, Training, and Education	1.00	0.67	0.56		
4	Budget and Resources	1.00	1.00	0.81		
5	Life Cycle Management	1.00	0.89	0.83		
6	Certification and Accreditation	1.00	0.80	0.60		
7	Critical Infrastructure Protection	1.00	1.00	0.50		
8	Incident and Emergency Response	0.71	0.59	0.54		
9	Security Controls	0.77	0.44	0.37		

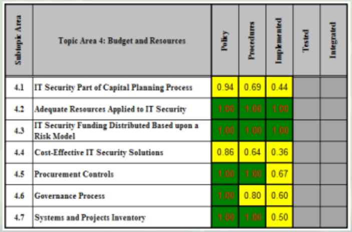
PRISMA is a transparent process that can show lower level detail

Before



Subtopic Area	Topic Area 4: Budget and Resources	Policy	Procedures	Implemented	Tested	Integrated
4.1	IT Security Part of Capital Planning Process	0.31	0.13	0.06		
4.2	Adequate Resources Applied to IT Security	🟥	🟥	🟥		
4.3	IT Security Funding Distributed Based upon a Risk Model	🟥	🟥	🟥		
4.4	Cost-Effective IT Security Solutions	0.36	0.36	0.21		
4.5	Procurement Controls	0.67	0.50	0.50		
4.6	Governance Process	0.40	0.10	0.10		
4.7	Systems and Projects Inventory	0.50	0.50	0.50		

After



Subtopic Area	Topic Area 4: Budget and Resources	Policy	Procedures	Implemented	Tested	Integrated
4.1	IT Security Part of Capital Planning Process	0.94	0.69	0.44		
4.2	Adequate Resources Applied to IT Security	1.00	1.00	1.00		
4.3	IT Security Funding Distributed Based upon a Risk Model	1.00	1.00	1.00		
4.4	Cost-Effective IT Security Solutions	0.86	0.64	0.36		
4.5	Procurement Controls	1.00	1.00	0.67		
4.6	Governance Process	1.00	0.80	0.60		
4.7	Systems and Projects Inventory	1.00	1.00	0.50		

Observations from Federal Agencies (1)

- Information security does not receive the needed attention by leadership, and it is one of many functions that compete for scarce resources only after meeting operational needs
  - Executive management is out of touch with the maturity of their security program
  - Executive management does not see cyber security as a major threat to mission accomplishment

- The organization has not developed a risk-based approach to information security based upon a clear understanding of threats to information and information systems

Observations from Federal Agencies (2)

- There is confusion between “compliance” and “performance”

- Management and system owners do not understand the information security actions for each stage of the system development lifecycle

- Organization has limited insight into what is being spent to support information technology or information security

Observations from Federal Agencies (3)

- The current system C&A process uses a "*one size fits all*" approach, and is dated

- The organization does not have an accurate inventory of the information assets

- Technical implementation, even for Enterprise security functions, is at the discretion of the local site or program management staff

Observations from Federal Agencies (4)

- External connections with collaborator or university systems to internal systems are in place with very limited or no management of these connections

Lessons learned from Federal Agencies

- Money spent on security is often not used properly or accounted for properly
  - Not a single agency considered the lost of public trust in the agency as a potential cost

- Executive management is often disconnected from what the security group is doing and is often surprised by the PRISMA grade
  - IT managers have learned how to game the FISMA report

Managements’ Reaction

- PRISMA results have traditionally indentified significant weaknesses in “real protection”

- Security management and practioners typically acknowledge and understand the results

- When informed of the PRISMA assessment results -
  - Executive management reaction is typical of someone hearing they have a fatal illness

Black Swan Effect and Security

- 5 stages of grief – These are played out when bad news is received

1. Numbness & Denial
2. Yearning & Anger
3. Organizational Despair & Sadness
4. Reorganization
5. Letting go and Moving on

In closing

- PRISMA provides a life cycle view of security to establish a program baseline
  - It can be rerun annually to gauge progress

- Security is a foundational process that must be integrated in with how business is done and equated with successful mission accomplishment
  - Integrate into the culture at all levels
  - Transparent

- When unexpected news is received
  - Don’t shoot the messenger – listen and evaluate
  - Stay the course -- Messengers need to be prepared to support the results through the initial phases of both denial and anger