PSM Security Measurement Working Group

26 July 2006

PSM Users Group Conference
Vail, CO

1

Meeting Objectives

- **Update** the group on SW Assurance Measurement efforts
- **Discuss** existing industry approaches for measurement and their applicability for SW assurance measurement
  - Differences
  - Overlaps
  - Harmonization among approaches
  - Potential use for SW assurance measurement
  - *White Space* or what needs are not covered by existing methodologies
- **Review** one of the available methodologies, GQM, and apply it to developing SW assurance goals for acquirers of SW services
- **Link** developed goals to metrics developed through ongoing PSM and SW Assurance Measurement WG
- **Solicit** feedback and ideas for next steps

2

Expected Outcomes

This Meeting
• Validate outcome of SW Assurance Measurement Workshop on July 20, 2006 • Solicit feedback from PSM stakeholder group • Provide input into the next SW Assurance and PSM meetings

Overall Effort
• Continue developing goals and measures for SW Assurance stakeholder groups • Collaborate with the PSM effort by contributing to guidebook on security measurement • Identify and develop an overarching comprehensive measurement approach that – Uses existing methods to the maximum extent – Addresses the *white space* that is not addressed by the existing measurement methodologies and ties methods together – Provides a means for organizing, structuring, quantifying, and interpreting large amounts of data originating from a variety of disparate sources from multiple stakeholders' point of view

3

Terms and Definitions (1 of 2)

- **Acquisition** – the acquiring of software development services or software products whether by contract or by other means, e.g., downloading open source software from the Internet. For the U.S. Federal government, also see the Federal Acquisition Regulation (FAR) Subpart 2.101(b)(2) definition of acquisition. In addition, for purposes of this document, "acquisition" applies to functions across the entire acquisition framework and the software development life cycle, including development, integration, testing, operations, maintenance and disposition, as well as the contracting/solicitation process itself. The contents are applicable to any type of software acquisition including commercial off-the-shelf (COTS) software purchases, custom developed software, system integration, services and outsourcing [Draft SW Security Acquisition Guide]
- **Asset** – anything that has value to the organization [ISO/IEC 13335-1:2004]
- **Assurance** – Grounds for confidence that a deliverable meets its security objectives [ISO/IEC 15408–1]
- **Assurance argument** – A set of structured assurance claims, supported by evidence and reasoning, that demonstrate clearly how assurance needs have been satisfied [ISO/IEC 21827]
- **Assurance evidence** – data on which a judgment or conclusion about an assurance claim may be based. The evidence may consist of observation, test results, analysis results and appraisals [ISO/IEC 21827]
- **Control *(different from software control)* –** Means of managing risks, including policies, procedures, guidelines, practices, or organizational structures which can be of administrative, technical, or legal nature [ISO/IEC 17799]
- **Control *(in software)*** – something that guides the process (best practice)

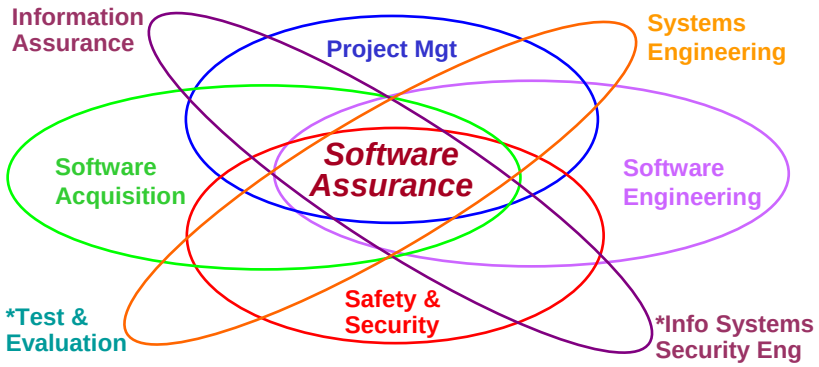
4

Terms and Definitions (2 of 2)

- **Information security** – Preservation of confidentiality, integrity, and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation, and reliability can also be involved [ISO/IEC 17799:2005]
- **Information security** – The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. [NIST SP 800-53; FIPS 200; FIPS 199]
- **Measure** - Variable to which a value is assigned as the result of measurement [ISO/IEC 15939]
- **Measurement** – set of operations having the object of determining a value of a measure [ISO/IEC 15939]
- **Risk** – The level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring [NIST SP 800-53; FIPS 200]
- **Safety** – is the state of being safe, the condition of being protected against physical, social, spiritual, financial, political, emotional, occupational, psychological or other types or consequences of failure, damage, error, accidents, harm or any other event which could be considered dangerous. Protection is from both the cause and from exposure to something that is not safe. It can include physical protection or that of possessions. Safety is often in relation to some guarantee of a standard of insurance to the quality and unharmful function of a thing or organization. It is used in order to ensure that the thing or organization will do only what it is wanted to do. [Wikipedia]

5

SW Assurance is supported by many disciplines



6

Each of which has a body of knowledge…

- **COBiT** – Control Objectives for Information and related Technology
- **COSO** – Committee of Sponsoring Organizations of the Treadway Commission
- **PMBOK** – Project Management Body of Knowledge
- **ITIL** – Information Technology Infrastructure Library
- **FIPS 199/200 and NIST SP 800 series** – Federal Information Processing Standards 199 (*Standards for Security Categorization of Federal Information and Information Systems*) / 200 (*Minimum Security Requirements for Federal Information and Information Systems*) and National Institute of Science and Technology Special Publication 800 series
- **ISO/IEC 27000 family** – Information security management system fundamentals and vocabulary
- **ISO/IEC 12088 etc** – Information technology -- Computer graphics and image processing -- Image processing and interchange -- Application program interface language bindings
- **ISO/IEC 15504** – Information Technology - Software Process Assessment
- **ISO/IEC 16085** – Software Engineering, Software Life Cycle Processes, Risk Management
- **CD ISO/IEC 27005** – Information security risk management
- **ISO/IEC 15408** – Evaluation criteria for IT security (a.k.a. Common Criteria)

Are there any other frameworks and standards you can think of?

7

…and a corresponding measurement method

- **ISO/IEC 15443** – Information technology -- Security techniques -- A framework for IT security assurance
- **CMMi** – Capability Maturity Model Integration
- **ISO/IEC 21827**– Systems Security Engineering Capability Maturity Model (SSE CMM) and associated International System Security Engineering Association (ISSEA) metrics work
- **NIST SP 800-55 and Draft SP 800-80** – National Institute for Standards and Technology Special Publication 800-55 (*Security Metrics Guide for Information Technology Systems*) and 800-80 (*Guide for Developing Performance Metrics for Information Security DRAFT*)
- **WD ISO/IEC 27004** – Information Security Management Measurements
- **ISO/IEC 15939** – Software Engineering – Software Measurement Process
- **PART/PMA** – OMB's Program Assessment Rating Tool and President's Management Agenda
- **Balanced Scorecard**
- **eSCM-SP and CL** – E-Sourcing Capability Model for Service Providers and E-Sourcing capability for Client Organizations
- Acquisition CMM
- SEI Operational Resiliency Model

Are there any other measurement methods you can think of?

8

There is also an abundance of requirements for security

- **GPRA** – Government Performance and Results Act
- **FISMA** – Federal Information Systems Management Act
- **Sarbanes Oxley** – Sarbanes-Oxley Act of 2002 or Public Company Accounting Reform and Investor Protection Act of 2002
- **HIPAA** – Health Insurance Portability and Accountability Act of 1996
- **Basel II** – Convergence of Capital Measurement and Capital Standards - A Revised Framework
- **California SB1386** – California Senate Bill 1386
- **OECD Guidelines on Internet Security** – Organization for Economic Co-operation and Development Guidelines on Internet Security
- **FFIECC Guidelines** – Federal Financial Institutions Examination Council's Guidelines
- **Federal Acquisition Regulation (FAR) –** Changes enacted 30 Sep 2005 changes that implement information security provisions of FISMA to all phases of IT acquisition life cycle

Are there any other laws, regulations, or guidance you can think of?

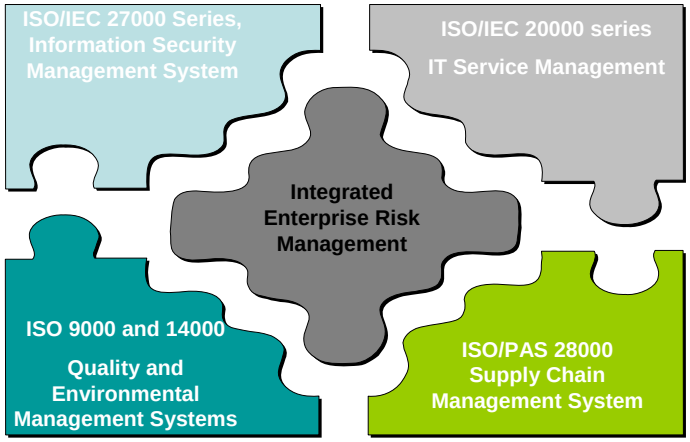
9

Efforts to harmonize these approaches are under way

- ISO
  - Several Management System series or families of standards have been developed or are currently under development
  - Specific standards are being harmonized across subject matter boundaries or within the same subject matters
- Industry organizations
  - SEI Operational Resiliency Model
  - ITQSC eSourcing CM Model
- Other models are integrated by individual service providers
  - CMMi and ISO/IEC 21827
  - ISO/IEC 17799 and CMMi
  - ISO/IEC 17799 and ISO/IEC 21827
  - ***Have you seen other examples?***

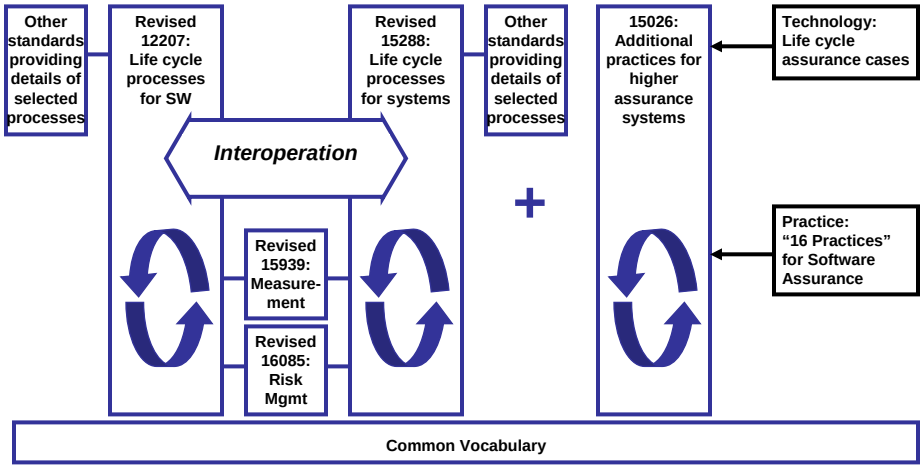
10

Management Systems use the same PDCA process



11

SC7 Harmonization



12

SC7 and SC27 Harmonization

- ISO/IEC 21827 revision
  - Strengthened references to measurement and added explicit measurement language
  - Annex A (Normative) Generic Practices replaced with reference to 15504-2
  - New Annex D (Informative) - contains original contents of Annex A for backward compatibility
- ISO/IEC 27005 development
  - Included references to ISO/IEC 16085 and ISO/IEC 21827
- ISO/IEC 27004 development
  - Uses many terms and definitions from ISO/IEC 15939
  - Leverages information model from ISO/IEC 15939 and tailors it for information security

13

Acquisition Goals Breakout Session

- Addressed the following questions:
  - Who are the SW Assurance acquisition stakeholders?
  - What would these stakeholders want to know about the ***products*** and ***services*** they are acquiring?
- Identified and documented at least 5 goals for each stakeholder group

14

Acquisition Goals – Enterprise

1. Customer Satisfaction – 95%
   - Sustainability
   - Maintainability
   - Reliability
   - Availability
   - Performance
   - Security
   - Functionality
2. Sustainable secure infrastructure
3. Manage/Raise market expectations
4. Stakeholder Satisfaction – 99%

Notes

- Data collection surveys must be designed appropriately to data granularity. Open ended questions on a survey provide a lot of insights
- Data needs to be normalized to be interpretable and useful
- Validate what you get with other source of measurement
- Stakeholder satisfaction is higher percent then customer satisfaction because stakeholders are a smaller group
- When defining goals be careful to be realistic. The last tenths of percent may cost lots of money.

15

Acquisition Goals – Developer

- Metrics for risk-informed GO/NOGO decisions in the software development lifecycle.
  - Rank Threats
  - Document what was done
  - Conduct quality checks based on documentation and artifacts – make risk based decisions teach phase of SDLC
- In Operation/in the field
  - Need a mechanism for reusing the tool as an attack vector
  - Zero ambiguity about operational status of the system

Notes

- Q: Is the structure the same for each application?
- A: The structure is tailored according to what the application is doing. (i.e. inputs/outputs, functionality…etc.)
- Metrics for risk-informed decisions in the SDLC provide the primary determining factor. Other goals would align with this goal, including higher reliability for users, better response to ide identified threats throughout the SDLC by developing more secure code and more comprehensive inclusion of security in quality checks. At that point, the decision maker will look at the documentation and the data and will make the decision.

16

Acquisition Goals – Service Providers (ISPs)

1. Confidentiality – provide secure communications for customers as in Defense in depth
2. Integrity – No theft of service, Only authorized service and ports
3. Availability - I/O, Maximize performance/cost
4. Detect malicious or unwanted activity quickly
5. Protect customer data
6. Filter correctly
7. Protect from unauthorized service
8. Have the right data for measurement
9. Measures - Sensors per node, False positives
10. User requirements define process for security/risk tolerance

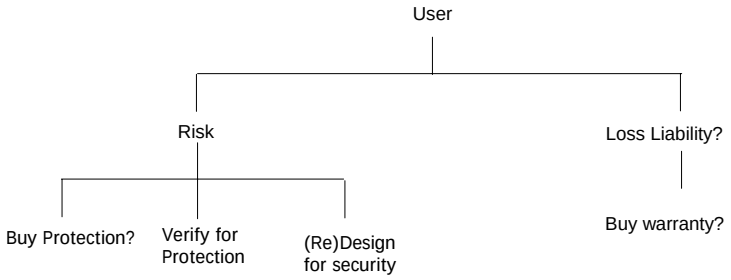
Notes

- Security is a sub-set of reliability; there should be no security-related surprises.
  - Q: How do you define security under reliability?
  - A: Security is at an equal level.

17

Acquisition Goals – User

1. To know the risks this product (P) exposes me to
2. To know the liability I may be exposed to, from using P
3. To define my security requirements
4. To verify the level of security achieved
5. To have my interests represented; my risks & liabilities limited
6. To know what I should do, to be a "good citizen"



18

Acquisition Goals – Vendor

- Meet internal deadlines
- Be realistic about expectations within technology life cycle
- Understand organization's strengths and weaknesses in SW assurance
  - What training does the staff need
  - What expertise we need to acquire
  - Are my projects staffed with appropriate staffing mix
- Match SW assurance capabilities against appropriate market need
  - What are security needs of the customer?
  - What capabilities do we have?
  - What is the cost to acquire various capabilities?
- Identify market need for SW Assurance capabilities
  - How do I gain a competitive advantage in SW assurance
- Assign sufficient staff to guarantee that deliverables will be met and would appropriately address SW assurance needs
  - How do I assign people to leverage their expertise in the future
  - How can I reuse products and resources from this project to the future project
- Make progress in security
- Avoid instances from data compromises caused by vendor product / minimize bad publicity
- Maintain / enhance vendor reputation in SW assurance
- Differentiate from competitors by making assertions that the competitors will not be able to make
- Integrating SW assurance into development process in a cost-effective manner
- Timely collaboration with customers to facilitate clarity of requirements specific and timely
- Minimize risks created by vendor software
- Ongoing collaboration w/customers (visibility into fielded use and .for future de development

19

Why measurement toolbox?

- Each measurement approach provides value
  - Presents the problem from a particular stakeholder group view, including their goals, measurement targets, and work practices
  - Provides a variety of insights into technical and behavioral aspects of SW assurance
  - Solves a piece of measurement puzzle
- If we can figure out how the existing measurement methods relate and what they don't cover we can
  - Provide a translation mechanism that will allow different stakeholder communities to **understand each others' measurement approaches and results**
  - Efficiently deal with compiling a long list of measures by **incorporating measures originating from other measurements approaches**
  - Allow stakeholder communities to continue using their methods and expand their view into measurement
  - Identify what is not covered and still needs to be developed

20

Different specs cover much of the same ground

NOTIONAL

ISO/IEC 15939	NIST SP 800-55	NIST SP 800-80	GQM
Information Need	• Performance Goal • Performance Objective	• Strategic Goal/Objective • Information Security Goal • Control Question • Control/Control Enhancement	Goal
Indicator/Interpretation	Indicator		Indicator Question
Derived Measures	Metric	Metric	Measure
Measurement Function	Formula	Formula	
Base Measure	Metric	Metric	Measure
Measurement Method	Data Source	Information Source	
Attribute	Implementation Evidence		
	Frequency	Frequency	

21

Tying Goals to Measures Breakout Session

- Addressed the following question:
  - Which of the measures in the ICM table fit the goals the we just developed
- Activities
  - Identified metrics in the ICM table that are appropriate for your goals/stakeholder combinations
  - ***Measures demonstrated accomplishment of goals***
  - Identified additional measures if needed
- Results
  - Updated ICM table
  - Other measures on the next slide

22

Additional Measures – Enterprise and Service Provider

- Qualitative subjective data is best measure
- Technology effectiveness – need to start with clean sheet of paper and need to start over
- General comments on Process Provision – sometimes need an actual # not a percentage (i.e. if 3 vulnerabilities on 40 node network vs 400 node network your risk is still the same)
- Least privilege and separation of duties need to be defined separately
- Need to include checks for those that have physical access only
- Recommend dedicated log server

23

Additional Measures – Developer

Category	Measures
Schedule	All
Cost	All
Size	All (design requirements)
Service Stability	No (Service provider)
Environment Properties	? (Design Spec.)
Product Quality	All
Service Quality	? (maintenance and feedback)
Progress Perform -system development -Service provision	? (Developer only at organizational level)
Technology Efficiency	All
Customer Satisfaction	? (Organizational level only)

24

Additional Measures – Vendor

- Vendor goals mapped across the ICM table
- Goals not mapped to table:
  - Timely collaboration with customers to facilitate clarity and of requirements - specific and timely
  - Ongoing collaboration with customers
  - Make progress in security – baseline/tread analysis (defects, etc).

25

Additional Measures – Users

- Noted that current ICM table has a customer satisfaction section but it overlooks the fact that customer is not always the same as the user.
- Quite difficult for the user to have any quantified view of the risks that they are exposed to.
- However, the user is the only one in position to make judgment as to what the product is being used for. So only user can judge/assess the USE of the product.
- On the other hand, the user is not in position to note any detail on the product so maybe have a consumer group approach to accrediting to products that have some verifiable level of security. (not in technical way, more in consumer group way).
- Liability issues: Governmental or society issues. Users can't react on their own. Need means to limit liability.
- Need means of encouraging users to be good cyber citizens.
- Product will tell you what it "can do" but not tell you what it's "for"
- "we have car & driver but we don't have consumer reports for the IT world"

26