SwA Measurement Framework Refresh

December, 2010

Why measure???

"*The only man I know who behaves sensibly is my tailor; he takes my measurements anew each time he sees me. The rest go on with their old measurements and expect me to fit them*."

- George Bernard Shaw

Source: www.CartoonStock.com

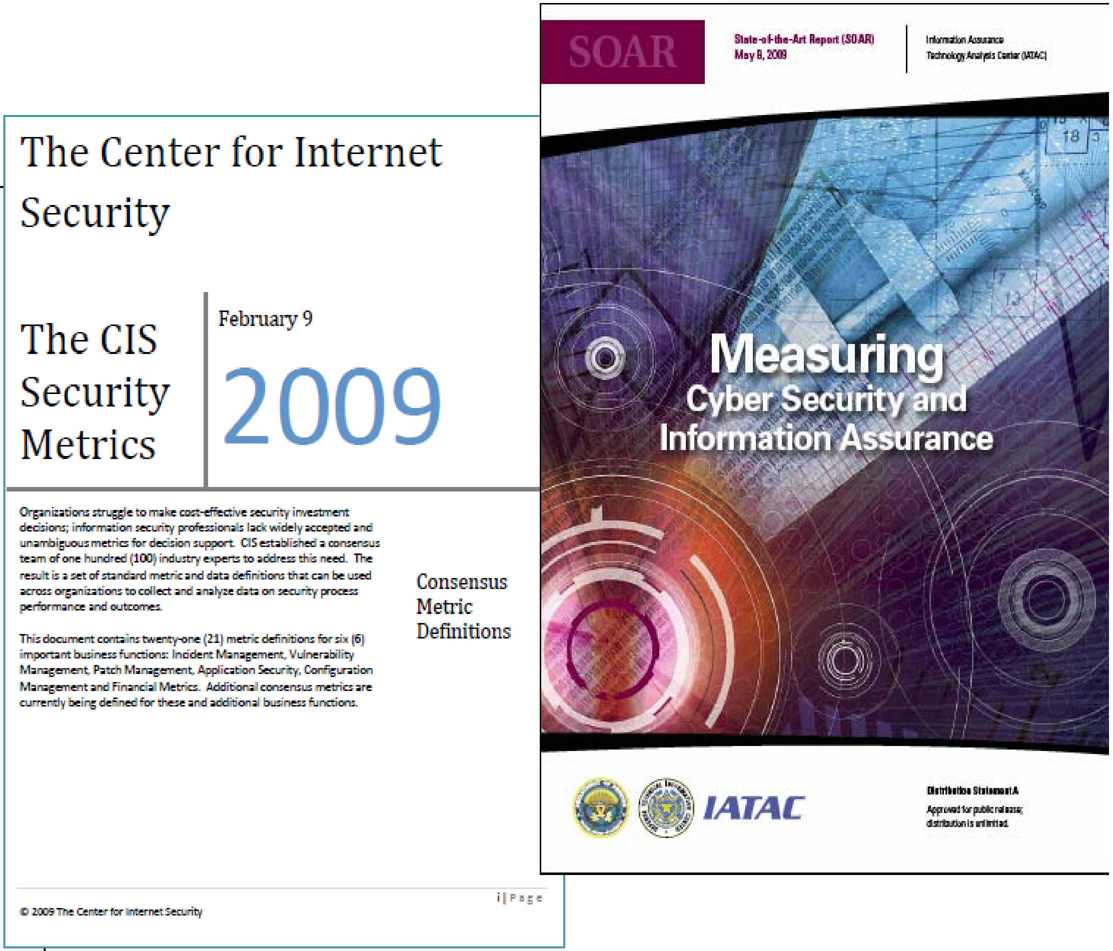
Standards and Best Practices

- NIST SP 800-55 Rev1, Performance Measurement Guide for Information Security
- ISO/IEC 27004, Information Security Management Measurement
- ISO/IEC 15939, Practical Software and System Measurement (PSM)
- CMMI Measurement and Analysis Process Area
- CMMI Goal, Question, Indicator, Measure (GQIM)

Industry Methodologies and Anthologies

Practical Measurement Framework for Software Assurance and Information Security

Oct 2008



The Center for Internet Security

The CIS Security Metrics

February 9

2009

Organizations struggle to make cost-effective security investment decisions; information security professionals lack widely accepted and unambiguous metrics for decision support. CIS established a consensus team of one hundred (100) industry experts to address this need. The result is a set of standard metric and data definitions that can be used across organizations to collect and analyze data on security process performance and outcomes.

This document contains twenty-one (21) metric definitions for six (6) important business functions: Incident Management, Vulnerability Management, Patch Management, Application Security, Configuration Management and Financial Metrics. Additional consensus metrics are currently being defined for these and additional business functions.

Consensus Metric Definitions

© 2009 The Center for Internet Security

i | Page

SOAR

State-of-the-Art Report (SOAR)
May 8, 2009

Information Assurance
Technology Analysis Center (IATAC)

Measuring
Cyber Security and
Information Assurance

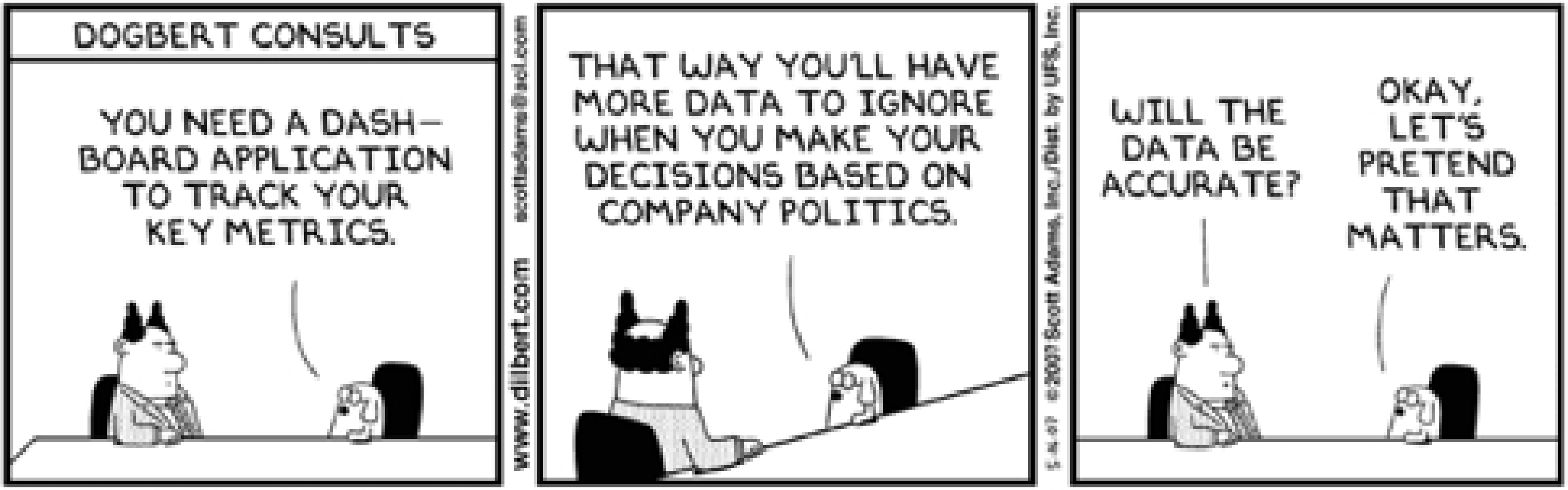
IATAC

Distribution Statement A
Approved for public release;
distribution is unlimited.

Success Factors and Expectations

- Obtain organizational acceptance and management commitment
- Ensure that IA performance measures program is manageable
- Ensure acceptable quality of data
  - Standardize data collection methods and data repositories
  - Standardize vocabulary and events reporting
  - Openly share information among organizational entities to ensure appropriate reporting
  - Use feasibility of data collection as one of the criteria for metrics selection
- Maintain long term focus
  - Manage expectations continuously
  - Iterate the program to measure critical things
  - Assign roles, train your responsible parties, and communicate that continuity is key for success

And it needs to be credible…


DOGBERT CONSULTS
YOU NEED A DASH-BOARD APPLICATION TO TRACK YOUR KEY METRICS.
scottadams@aol.com
www.dilbert.com
THAT WAY YOU'LL HAVE MORE DATA TO IGNORE WHEN YOU MAKE YOUR DECISIONS BASED ON COMPANY POLITICS.
5-6-07 ©2007 Scott Adams, Inc./Dist. by UFS, Inc.
WILL THE DATA BE ACCURATE?
OKAY, LET'S PRETEND THAT MATTERS.

© Scott Adams, Inc./Dist. by UFS, Inc.

Framework Overview

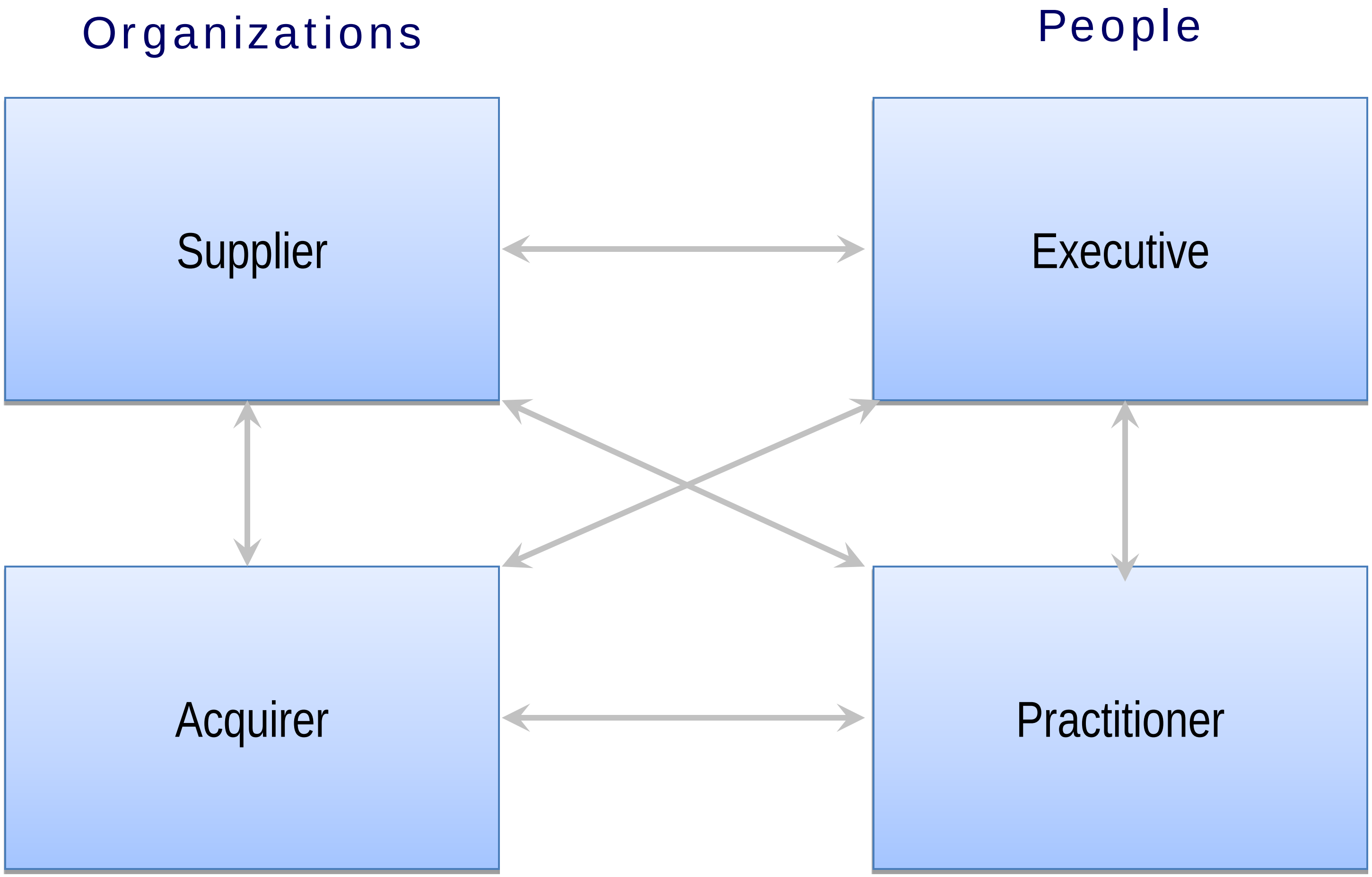
What it does

- Explains how to integrate SwA measurement into existing measurement approaches
- Provides a common framework for addressing SwA measurement regardless of currently used measurement approach
- References existing measurement body of knowledge for basic information on measurement approaches
- Explains a basic process for measurement that is common to referenced measurement methodologies
- Provides example goals/information needs and measures for the primary SwA stakeholder groups
- Contains measures based on common enumerations to get to tangible software-related items to measure

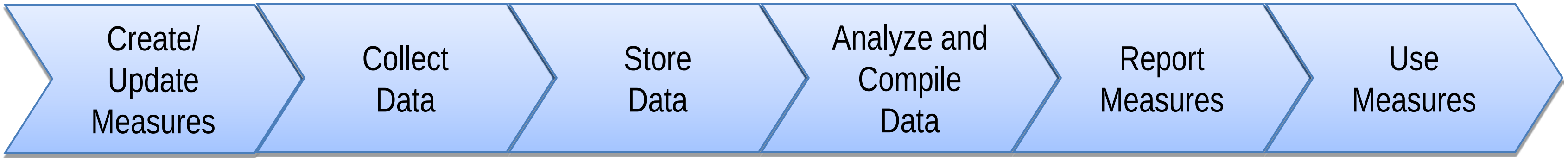
What it does not

- Create a new stand-alone measurement approach for SwA
- Provide a single text book for SwA measurement that can be used without referencing other methods
- List ALL possible SwA measures that could be ever needed by a project or organization

Stakeholders



Harmonized Measurement Process



Create/ Update Measures

- State goals
- Identify data sources and elements
- Analyze how goals and data elements relate
- Create a series of measures

Collect Data

- Gather data from available data sources

Store Data

- Document/ store data in an appropriate repository

Analyze and Compile Data

- Analyze collected data
- Compile and aggregate into measures
- Interpret data
- Identify causes of findings

Report Measures

- Document measures in appropriate reporting formats
- Report measures to stakeholders

Use Measures

- Support decisions
- Allocate resources
- Prioritize improvements
- Communicate to executives and external stakeholders

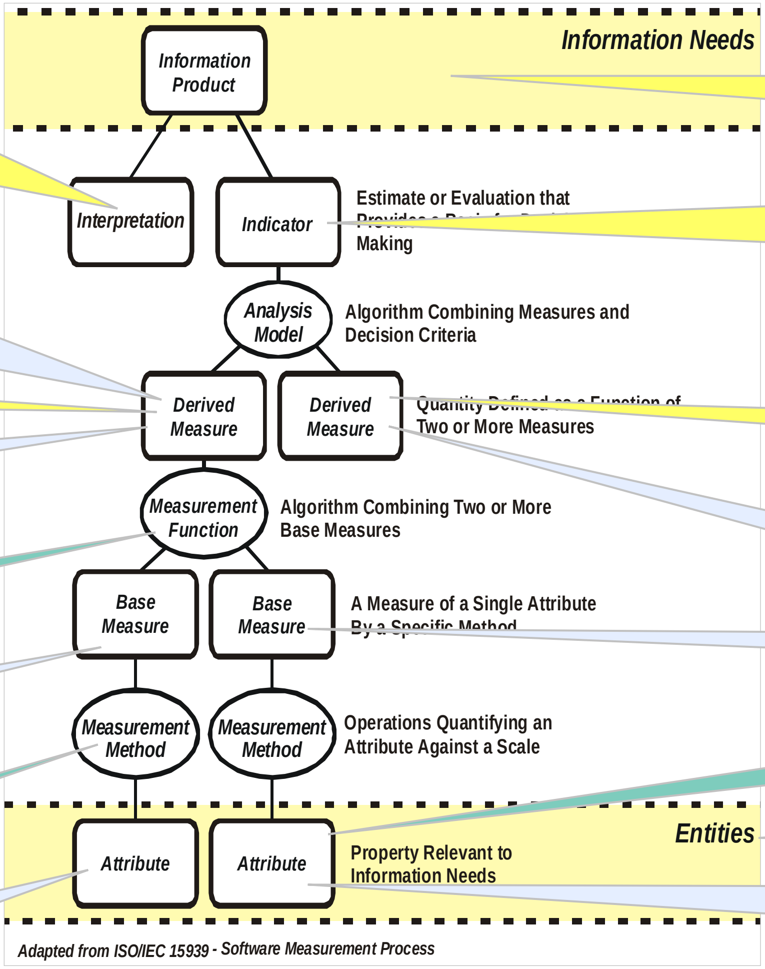
Continuous Improvement

- Refresh measures to ensure they are still relevant to the project, program, or organization
- Train measurement staff

SwA Measures Examples

- Acquisition
  - Number and percent of acquisition discussions that include SwA representative
  - Number and percent of contracting officers who received training in the security provisions of the FAR
  - Percent of documented Supplier claims verified through testing, inspection, or other methods
  - Number and percent of relevant high impact vulnerabilities (CVEs) present in the system
- Testing
  - Number and percent of tests that evaluate application response to misuse, abuse, or threats
  - Number and percent of tests that attempt to subvert execution or work around security controls
  - Percent of untested source code related to security controls and SwA requirements

Building measures and indicators


Information Needs
Information Product
Interpretation
Indicator
Estimate or Evaluation that Provides a Basis for Decision Making
Analysis Model
Algorithm Combining Measures and Decision Criteria
Derived Measure
Derived Measure
Quantity Defined as a Function of Two or More Measures
Measurement Function
Algorithm Combining Two or More Base Measures
Base Measure
Base Measure
A Measure of a Single Attribute By a Specific Method
Measurement Method
Measurement Method
Operations Quantifying an Attribute Against a Scale
Entities
Attribute
Attribute
Property Relevant to Information Needs

Adapted from ISO/IEC 15939 - Software Measurement Process

Trend of CVEs with high CVSS scores against maturity levels indicates a relationship between maturity level and CVSS scores

CVEs present on the system with CVSS score above 7

EAL Rating

Number of or CWEs per set number of lines of code

Measurement Process

Number of CVEs or CWEs

Measurement

Line of code

Understand the impact of improved assurance practices

Comparison of CVEs with CVSS scores above 7 compared with project's Maturity Level

CMMI Maturity Level

CVSS Score

Number of lines of code

MOF Element

Measured Artifact

CVE/CWE/defect

How to Begin

Start Small

- Expand your project cost, schedule, quality, and growth measures to cover SwA
- Start with a manageable, small set of SwA measures
- Leverage existing industry lists and select applicable measures
- Use the framework to translate measures from industry lists into your organization’s approach
- Add more SwA measures as the project learns
- Train data collectors to apply their knowledge to SwA or train SwA/security staff

Measure Behavior

- Measure process behaviors as well as results
- Take advantage of unintended consequences produced by process measurement
- Identify and measure best and worst practice behaviors as well as results

Get Management Support

- Obtain tangible support for SwA measures development and use at every management level
- Maintain support through regular reporting to stakeholders, tailored to their levels
  - Address their goals
  - Reduce detail further up the management chain

Incorporate SwA measures into your existing measurement activities