Reproducible Measurement as a Foundation for Security Assessment Metrics

John Nye

Metricon '09

August 11, 2009, Montreal

“How’m I doing?”

– Former New York City Mayor Edward I. Koch, ca. 1978[1]

[1] Jaquith, A., *Security Metrics, Replacing Fear, Uncertainty, and Doubt* (Upper Saddle River, NJ: Addison Wesley, 2007) 251.

So, you conduct an assessment...

ISO

ITIL

COBIT

BITS FISAP

PCI

Internal Assessment

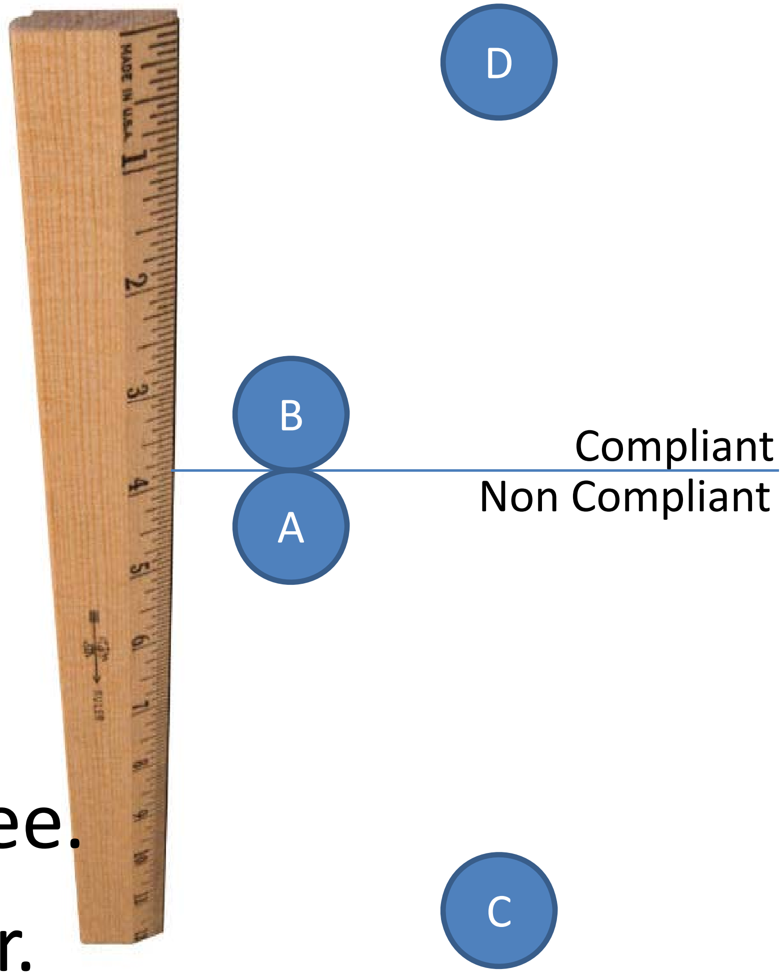
SAS-70

Findings

Compliant/
Not-Compliant

In Place/
Not-In Place

Unqualified/
Qualified



- There is a matter of degree.
- But, we don’t have a ruler.
- I’m proposing to define what an inch is.
  - Or rather, what <u>each</u> inch is.

Examples of Standardized, Subjective Measurement for Objective Comparison

- Humanities Grades

- Figure Skating

MEASUREMENTS OF DEGREE

CMM as a Model

- CMM 0 – No control activity

  0 points
- CMM 1 – Process happens but not repeatable

  40 points
- CMM 2 – Process documented and repeatable

  65 points
- CMM 3 – Qualitative measurement

  85 points
- CMM 4 – Quantitative measurement

  95 points
- CMM 5 – Continuous improvement feedback

  100 points

Example: Policy

Policy Document (Attribute List)

- No Document

  0 points
- Document Exists

  + 50 points
- Business Alignment

  +20 points
- Includes or references technology standards

  +30 points

Policy Review (CMM-like)

- Level 0

  0 points
- Level 1

  50 points
- Level 2

  75 points
- Level 3

  85 points
- Level 4

  95 points
- Level 5

  100 points

Example: Intrusion Detection

IDS Deployment (Design Maturity)

- Perimeter IDS Sensors

  +20 points

- IDS Logging

  +20 points

- Automated Alerts

  +30 points

- Interior IDS Sensors

  +15 points

- HIDS in DMZ and on Critical Servers

  +15 points

Example: Workstation Security

Host Configuration (Attribute List)

- No local admin/root
  +10 points
- Running AV
  +25 points
- Service minimization
  + 10 points
- UI Times Out
  +10 points
- PW Policy Enforced
  +10 points
- Etc.

Build Process (CMM-like)

- Level 0
  0 points
- Level 1
  0 points
- Level 2
  75 points
- Level 3
  90 points
- Level 4
  95 points
- Level 5
  100 points

Isn’t this a solved problem?

- Partly
  - Most GRC tools can assign points to control attributes and generate weighted scores.
- The gaps:
  - “Sufficiency” based with no description of “degree”
  - Non-portable
  - No context for complexity
  - No context for veracity of data
  - I’m not aware of any standard that addresses design maturity / comprehensiveness.

METRICS & CONTEXT

Security Assessment Metrics:

Requirements

- Scoring method divorced from assessment standard
- Comprehensive in breadth
- Reproducible
- Assessment / standard agnostic
- Wide use

Helpful Ideas

- We don’t have to measure everything
- We’re measuring “Control Quality” not risk
- Scores are not findings
- Subjectivity should be baked into the measurement standard, not interpreted upon application

Proposed Metrics

- Control Quality
- Adjusted Control Quality
- Score Veracity

Control Quality

- Overall Score
  - Control Area Scores (i.e. ISO 27002 chapters)
    - Control Scores
      - Descriptive Classification
- Descriptive Classification:
  - Policy Review
    - Level 2: Policy has been reviewed and comments provided by someone other than the author.
    - Level 3: Policy has been reviewed by technical subject mater experts and those opinions have been provided to an executive for final approval.
    - Level 4: In addition to Level 3, policy exceptions and violations are reviewed quarterly

Adjusted Control Quality

- Environment Complexity
  - Low
    - 1 site, <150 hosts
  - Medium
    - <5 sites, <1500 hosts
  - High
    - Everybody Else

- Proposed for adjusting
  - Processes scores
  - Governance scores
  - Manageability scores

“CMM”	Low	Medium	High
0	0	0	0
1	75	50	0
2	80	75	0
3	90	85	75
4	100	95	90
5	100	100	100

Score Veracity

- High – Assessment conducted against a recognized, peer-reviewed ISMS standard according to AICPA criteria.
- Medium-High – “2 Week” security assessment, i.e. PCI
- Medium – 1 to 3 days of analysis, single site visit
- Medium-Low – Questionnaire + Phone Call
- Low – Self Assessment Questionnaire

The Tuple

- Control Quality = C
- Adjusted Control Quality (medium size firm) = B
- Score Veracity (Moody’s) = Medium-High

NEXT STEPS

Work to Be Done

- Working Group
  - Agreed upon descriptions
  - Weights and Measures
  - Peer Review
  - Home for Publication
  - Adoption

Thank you

John Nye

jnye@jnyesecurity.com

(617) 501-3248