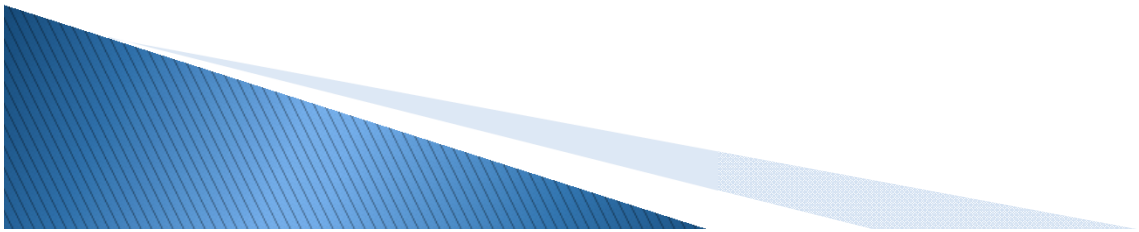
AW-IT-01 Methodology

(Cybersecurity Performance Index)

Updated April 2019



Outline

AW-IT-01

- Context
- Purpose/Approach
- Alignment
- Composite vs. Multiple Metrics
- Composition
- Calculation (Back-up slides)

Context

AW-IT-01

Why a security metric? To measure adherence to Federal law and NRC policy, and to reduce information technology risk to NRC mission.

- Increasing cyber threat & countless attacks against Federal agencies
- Numerous GAO and IG findings (OMB/FISMA required activities not completed, etc.)
- Management needed some way to quantify risk (*and progress of mitigating it*)
- What gets measured gets managed

CPI Complements NRC IT Risk Management Efforts

- Need to identify, understand, communicate, prioritize and mitigate risks
- Significant amounts of unquantified security data (and risk) within NRC
- Security data requires organization, visibility, attention to outstanding issues
- Distills thousands of documents/data points in ADAMS, security plans, tools, test reports
- Enables Offices/CIO/CISO to manage continuous monitoring & understand required activities

Purpose / Approach

AW-IT-01

Intent

- Positively influence behaviors contributing risk to NRC mission
- Be quantifiable, measurable, understandable and transparent
- Incorporate new data sources as they become available
- Incorporate additional components as risks change over time

Direct input to QPR, and is aligned with:

- FISMA -- Annual Cybersecurity Risk Management Activities Memo (CSRMA)
- Monthly Continuous Monitoring Status Reporting (CMSR) to ISSOs
- CIO daily situational awareness briefing
- FITARA briefings and methodology

Methodology

- Measurement: Quarterly, by Office/Region, Q4 becomes next FY baseline
- FY targets: 2% per quarter, 8% annual reduction*
- Threshold: Offices with a baseline of <= 30 need only to maintain it

(avoids minor increases in risk causing large % changes within Offices with scores close to zero)

* The 8% goal is due to several factors including: significant reductions in CPI have already occurred over the years and continued 10% improvement is increasingly difficult to achieve; 8% allows for uniform (integer) quarterly reduction targets; the fact that DHS/OMB/GAO have introduced additional requirements; and the NRC Perf Mgt System in FY17 could not display decimal percentages (e.g. 2.5%).

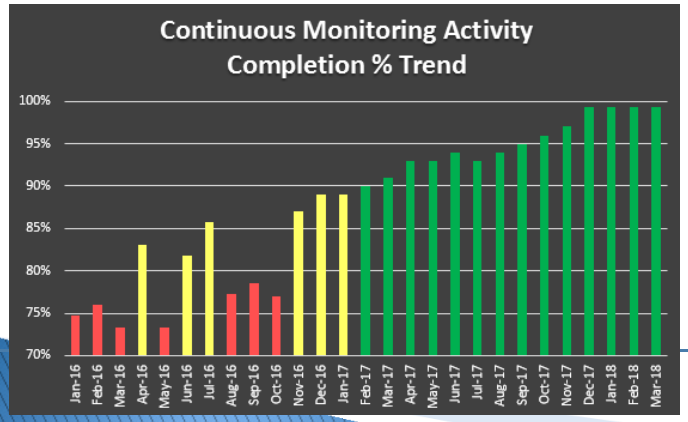
Alignment

AW-IT-01

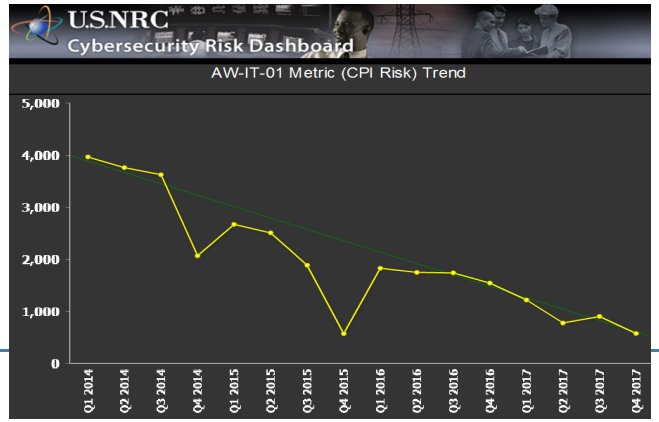
- Direct input to Quarterly Performance Reporting (QPR)
- Aligned to support Office staff, OMB FISMA requirements, and annual EDO/CIO direction

  (FY15-19 Cybersecurity Risk Management Activities Memo)
- Integrated into Executive training
- Leverages Configuration Non-Compliance metric currently derived in quarterly Federal Information Technology Acquisition Reform Act (FITARA) risk scoring
- Staff-level issues/challenges reviewed at monthly continuous monitoring mtgs
- CISO/Office-level discussions at periodic Cybersecurity Posture mtgs
- DEDOs review & question at Quarterly Risk Management briefings

Compliance is increasing…



… Measured risk is decreasing.



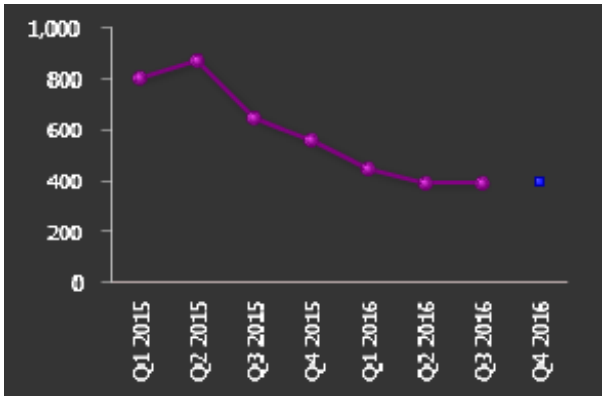
Why Composite vs. Multiple Metrics?

AW-IT-01

Advantages of Composite

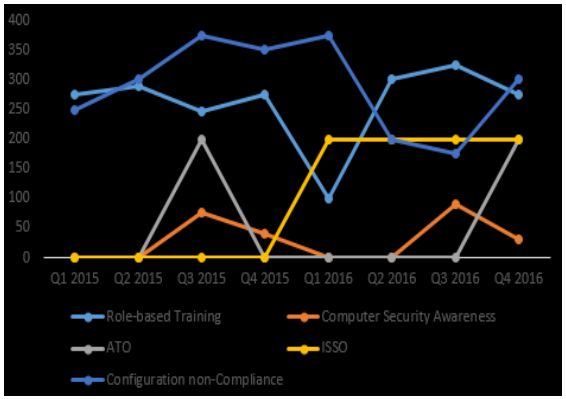
- Allows executives/staff to see at a glance what their security posture is (for those components measured)
- Allows executives/staff to more easily understand their *overall* risk trend
- Provides Offices flexibility to manage their approach to meeting targets:
  - Executives/staff can choose which components to focus improvement upon
  - Some components may not meet targets, balanced by others that may exceed
  - Multiple metrics would require *each* be tracked, measured, displayed & scored (R/Y/G)

Composite CPI



Vs.

Multiple Metrics



Composition

AW-IT-01

- The metric is a composite metric based upon four well known risk-drivers critical to minimizing risk to NRC mission
  1) Computer Security Awareness (CSA) training
  2) Role-based training (RBT)
  3) Continuous Monitoring (ConMon) metric (fmrly ITIM-OCIO-77)*
  4) FITARA Configuration Non-Compliance (CNC)*

Note that ConMon and CNC are only applicable to offices with authorized NRC IT systems (e.g. ADM, ASLBP, CFO, NMSS, NRO, NSIR, OCHCO, OCIO, RES, RIII, and RIV)

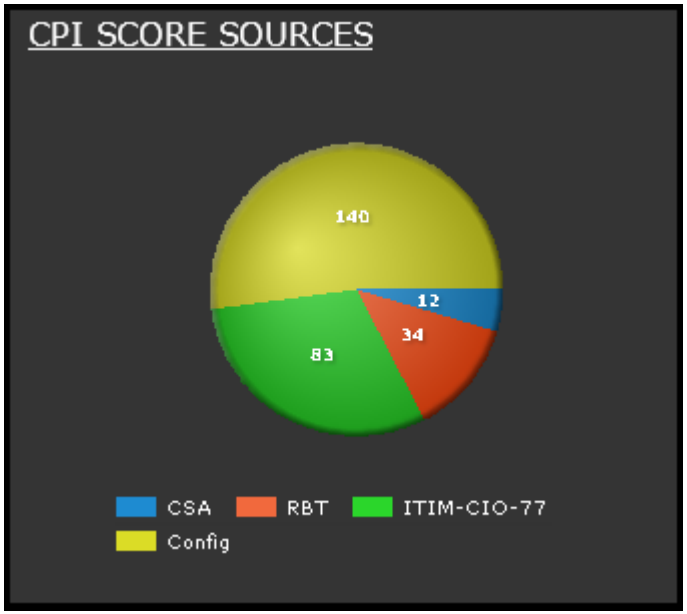
- Future metric composition can evolve in response to
  - Changing threats (e.g. OPM hack, Phishing attacks, etc.)
  - Improved data sources (e.g. DHS Continuous Diagnostics and Mitigation)
  - Desired behavior changes (replacing components where risk approaches zero with those requiring more focused risk mitigation efforts)

**ConMon measures the % completion of 10 required OMB/FISMA activities including: Contingency Plan (CP) Test, Periodic Security Control Assessment (PSCA), Vulnerability Assessment Report (VAR), System Security Plan (SSP), Information System Security Officer (ISSO), Authority to Operate (ATO), and Designated Approving Official (DAA) conditions. Note: In FY18Q4, Contingency Plan (CP) and Business Impact Assessment (BIA) were added in response to IG findings. Security Impact Assessments (SIA) were added in FY19Q1.*

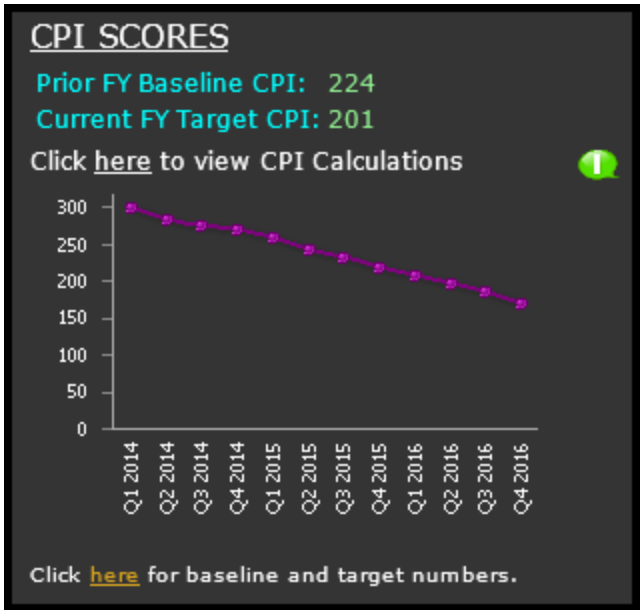
Composition

AW-IT-01

Example - shows relative sources of risk within an Office:



Same Office's trend over 2 years:



Backup slides

Calculation

AW-IT-01

- An Office's score is calculated continuously, and recorded at the end of each quarter (with Q4 representing the final AW-IT-01 for the FY)
- An Office's score is the sum of 4 risks: CSA + RBT + ConMon + CNC
- Similarly, the Agency score is the summation of all Offices' scores

Where:

Acronyms are defined on previous pages

1. CSA risk = Quarterly target % - Current actual completion %

   Target %'s are: Q1&Q2 = 0%; Q3 = 30%; Q4 = 96%. The actual % is taken from OCHCO website

2. RBT risk = Target (96%) – Current actual completion %

   Actual % = #roles trained/#roles requiring training (source: OCIO tracking spreadsheet)

3. ConMon risk = % of Risk Management Activities due (but not completed) by current date

   Activities include: CP Test, PSCA, VAR, SSP, ISSO, ATO, BIA, CP and DAA Conditions (and SIA in FY19)

4. CNC risk is taken from established quarterly FITARA scoring, and is based upon weighted # of configuration risks from most recent system scans.

   For CNC scoring methodology, please contact OCIO/GEMS/CSO for the latest guidance.

Due to large numbers, CSA and FITARA CNC are weighted .5 and .05, respectively. Note: as of 19Q2, CNC is no longer weighted due to greatly reduced numbers resulting from the new FITARA methodology.

Sample Office -- 17Q3

Status: Green -- Q3 target of -6% (or better) reached

AW-IT-01

Component	Score	Calculation	Notes
Role-based Training	(target exceeded, no risk)	96% (target) - 100% (actual) = (target exceeded, no risk)	
Computer Security Awareness Training	**6.5**	30% (target) - 17% (actual OCHCO data) = 13%, x .5 = 6.5	*Target is 0% in Q1&2 (as training not available until late Q2), 30% in Q3, and 96% in Q4 (Aug 15), and is weighted by .5*
Configuration Non-Compliance	**12.0**	240 (sum of FITARA CNC scores for all systems in Office) * .05 = 12	*FITARA configuration scoring results in very large #s, thus weighted by .05*
Continuous Monitoring Activities (ITIM-OCIO-77)	**0.0**	100% (target) - 100% (actual %) = 0	
Total: *(may not add due to rounding)*	**18.5**	*Mitigation Strategy for Q3 - Status Green -- Q3 target of -6% (or better) reached. To meet the Q4 risk reduction target of -8%, achieve the Computer Security Awareness (CSA) training completion goal of 96%, maintain Role-Based Training (RBT) (currently 100% a/o 7/14/2017) and ITIM-OCIO-77, and FITARA Configuration Non-Compliance risk score must be no greater than 600.*	

Notes:

- Office ended FY2016 with an AW-IT-01 score of **30** (which became FY17 baseline)
- Since the FY17 agency-wide target is a 2% reduction/Qtr, in Q3 there should be a 6% decrease (or **30** * 94%) resulting in a Q3 target of **28.2**
- Comparing the Q3 score above against the baseline, results in a **-38.4% (a decrease)** in risk (**18.5 – 30**)/ **30**

Please see note on previous page regarding updated weighting of FITARA configuration risk.