Turning Your Mainframe from Securable to SECURE

Jim Ramsay
Vice President
Enterprise Information Security

September 22, 2015

IBM 2015 Fall z Systems Premier Event

The Problem

- Assumption that mainframes are secure
- Too narrow a focus on the ESM
- Not enough focus on the system components' configuration settings that can affect security
- Decisions affecting security made years earlier have never been revisited

The Solution

- A comprehensive detailed security assessment and remediation program
- Include any significant items that can affect the state of security on your mainframes

Program Overview

Defining The Program

- What can affect the state of security on your mainframe?
  - Security products (ACF2, RACF, Top Secret)
    - Global config parms, command prop., ESM DR plans…
  - System components
    - exits/calls, parms, STCs, JES…
  - z/OS system products
    - CICS, IMS, MQ, job scheduling…
  - System management tools from ISVs
  - In-house tools and utilities

Risk Ranking

- Evaluate topic areas based on potential for exposures impacting system/data:
  - Confidentiality
  - Integrity
  - Availability
  - Auditability
- Evaluate potential impacts to the company's:
  - Financials
  - Reputation

Prioritizing

- Now that you have risk rankings based on something other than collective gut feel…
  - Prioritize your Program's work
  - Won't always be purely highest risk first

- Will need to consider other relevant factors
  - Other projects affecting same target area
  - Some projects may need to fund the involvement of others, some projects may not
  - Availability of particular SME(s)

Methodology

- Selection
- Assessment
- Remediation
- Post-implementation verification (PIV)
- Project review/lessons learned
- Risk Management / Audit reviews (if applicable)

Necessary Tools

- Access Discovery
  - Identify access activity/attempts
  - Non-disruptive
- Data Analysis
  - Feature-rich, reliable, easy to use vendor supported tools
- System Security Changes
  - Prevent regression in real-time
  - Undercutting prevention
  - Auto-populate known/pre-established permissions
  - Simplified processes

Necessary Tools, cont'd

- Benefits
  - Time spent doing data mining / analysis dramatically improved
  - Avoids headaches and time commitment associated with home grown tools
  - Quality / reliability of work due to thoroughly QA'd tools
  - Easy to use
  - Prevents rework due to regression avoidance
  - Prevents issues with undercutting
  - Efficiency gains from auto-populating permissions
  - Use of out-of-the-box functions translates to fewer, more straightforward steps to accomplish tasks

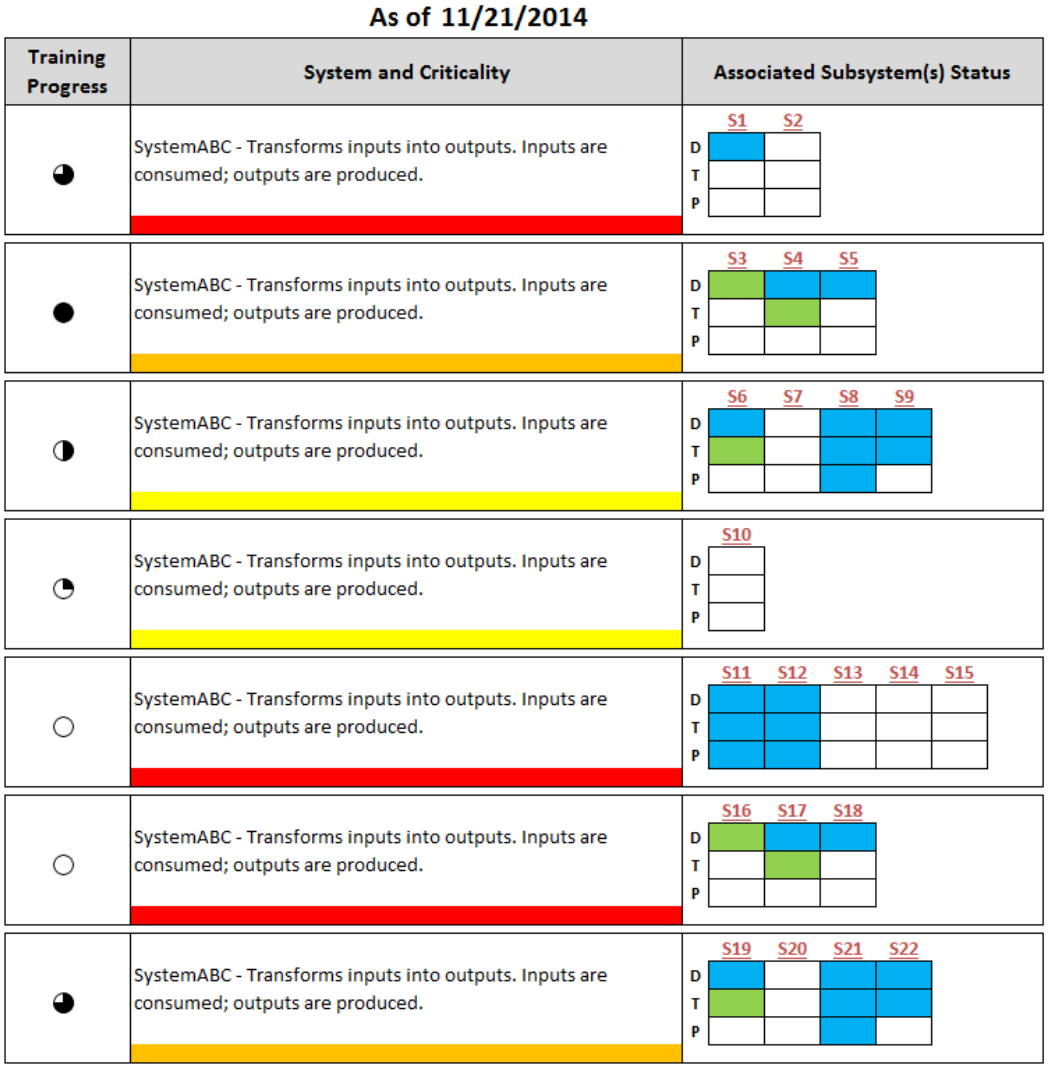
Program Management

Managing the Program

- Startup
  - Leadership briefings –articulate the risk in business terms
  - Overcoming the doubters – i.e., “show me”
- Stakeholder briefings
- Funding
- Communicate, communicate, communicate!
  - Multiple audiences, different messages
  - Numerous methods

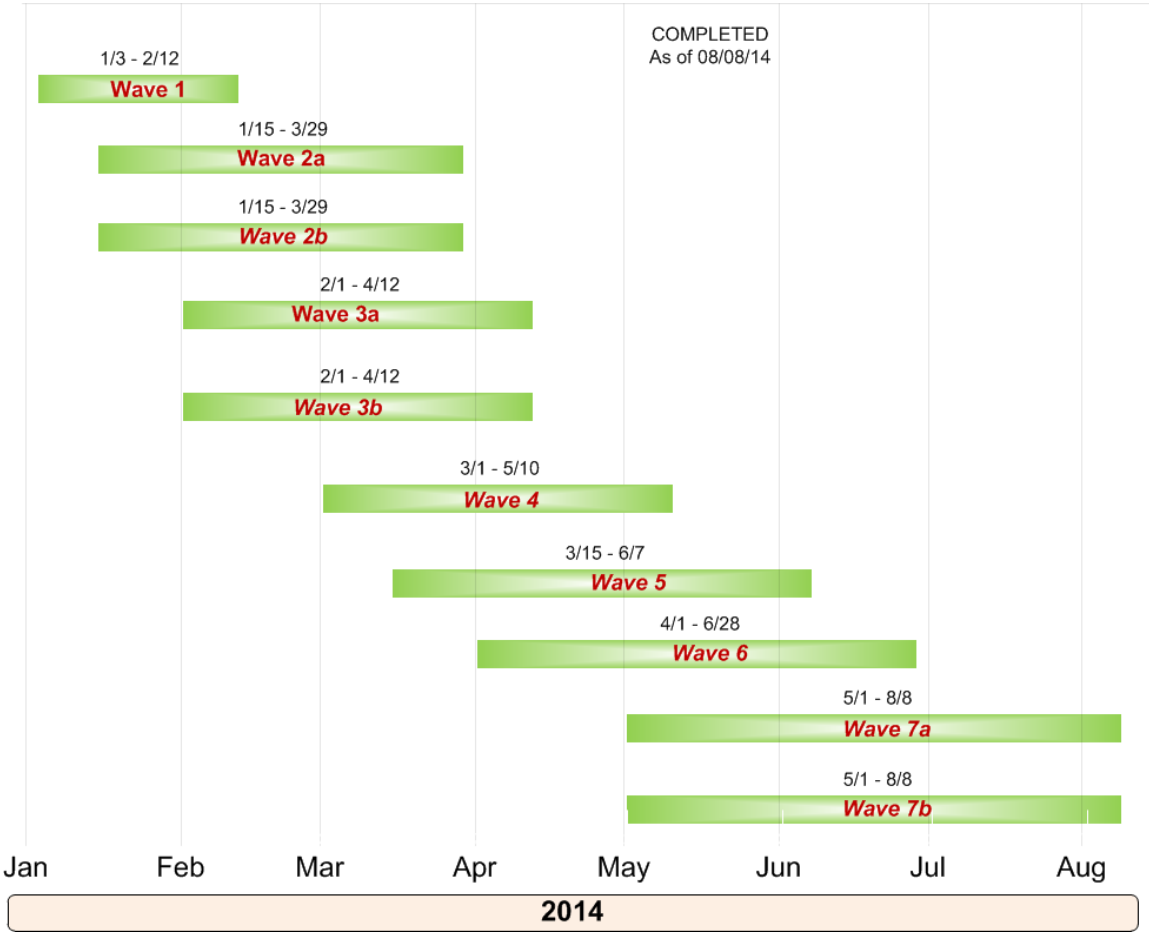
Dashboards

- Internal dashboards with detailed project progress
  - Started, in progress, or completed
  - Status by phase: Design, Testing, Production
  - Risk level (H/M/L) of associated risk



Project-specific Progress Charts

- Useful for very long-running remediation tasks
  - Same task affecting hundreds of applications
  - Timeline measured in quarters rather than weeks or months



Metrics

- Summary Metrics
  - Rollup of data from detailed dashboards, merged with project schedules