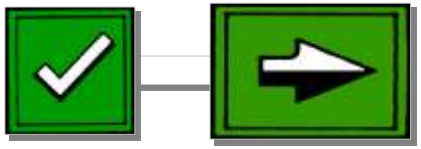
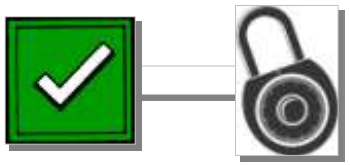
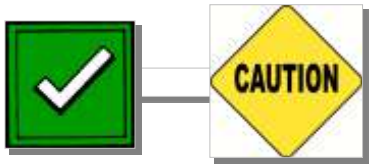


Role of SCAP in an Emerging Strategy for Continuous Certification and Accreditation

Kim Watson, NSA/IAD
Jim Ronayne, NSA/IAD
Dr. George Moore, DoS IRM/IA

September 2010



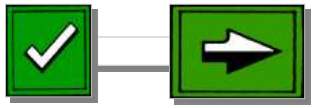


How can Federal Agencies leverage their successful Certification and Accreditation Programs?

- **…to increase the frequency of monitoring by a factor of 50 to 300?**
- **…to measurably increase security?**
- **…to do so using existing C&A Budget flows?**

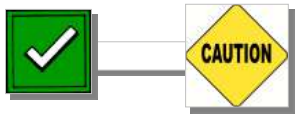
How can SCAP be used to facilitate this process?

…express what needs to be checked.



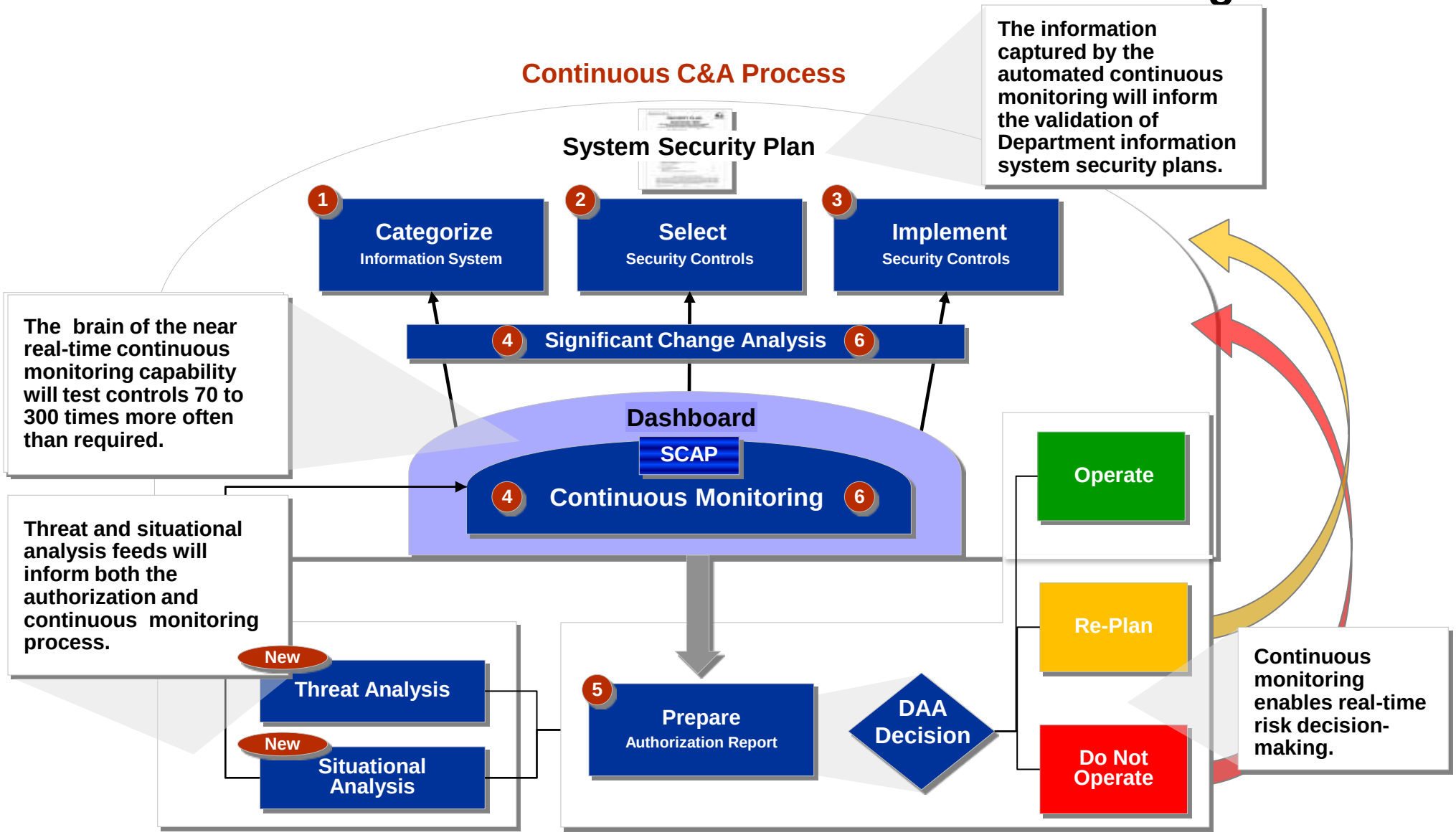
…express results and drive follow-on activities.

…express results in terms of (mapped to) controls.



…help associate threat and impact to the vulnerability results.

The Department's continuous C&A process adheres to NIST rules and achieves near real-time monitoring



The continuous monitoring dashboard is the brain of near real-time C&A

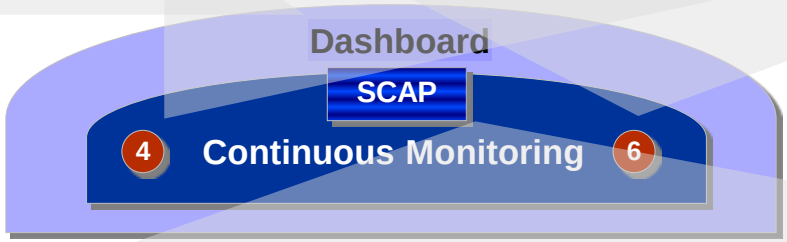
Continuous Monitoring Process

NIST's steps 4 and 6 are really both about testing.

- Step 4 involves testing during "certification" and
- Step 6 involves testing during "monitoring"

These are really the same.

The dashboard can (eventually) provide documentation of testing of all controls in a way that is timely, targeted, and prioritized.

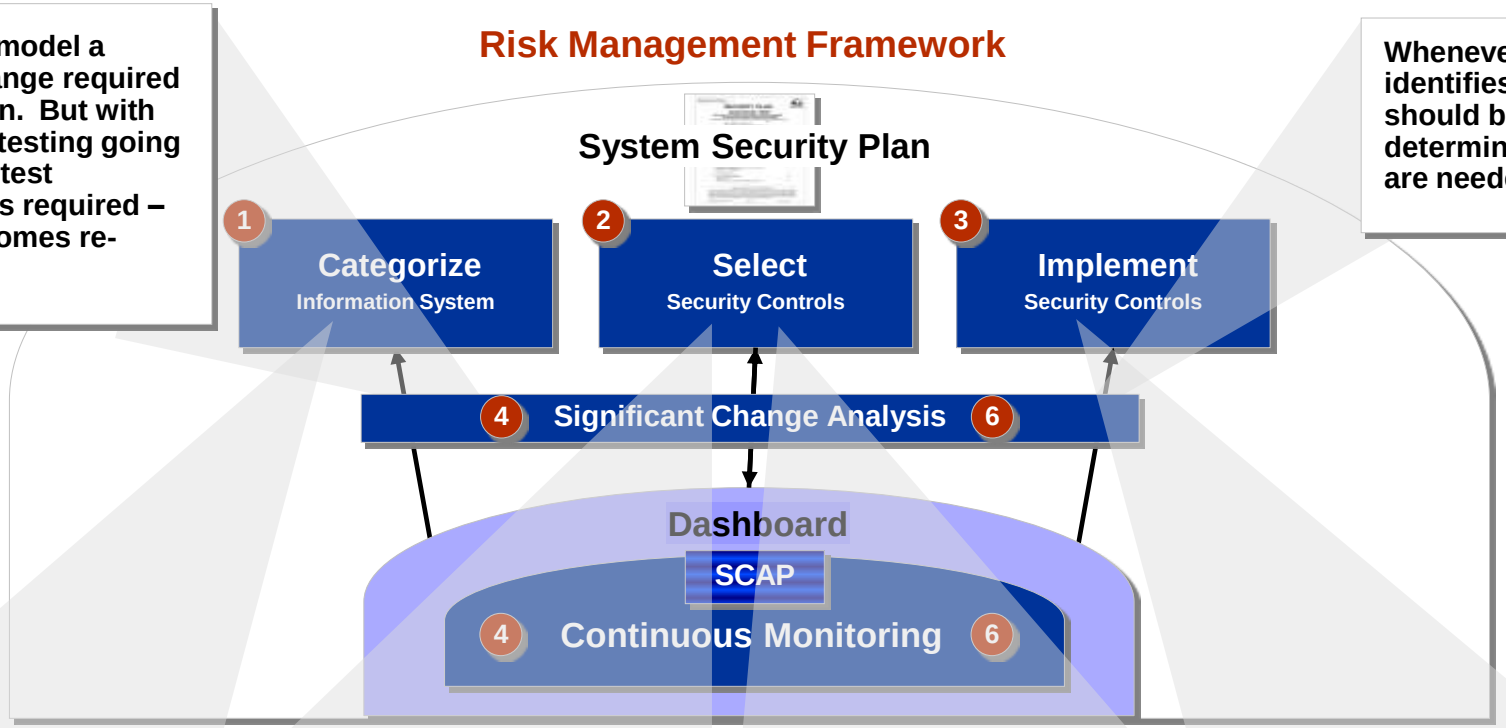


The SCAP language, provided by NSA, NIST, etc., should be used as the way for testing tools to communicate results to the dashboard. This provides many benefits including:

- Standardized language for conducting repeatable tests, and expressing test results in a re-usable format.
- Standardized re-usable content that can be borrowed from other agencies.
- Enabled comparison of test results for measurement and risk management.

The dashboard dynamically feeds the Risk Management Framework

Under the old model a significant change required a recertification. But with near real-time testing going on, no special test (certification) is required – The focus becomes re-planning.



Whenever the dashboard identifies issues, they should be evaluated to determine whether changes are needed to the SSP.

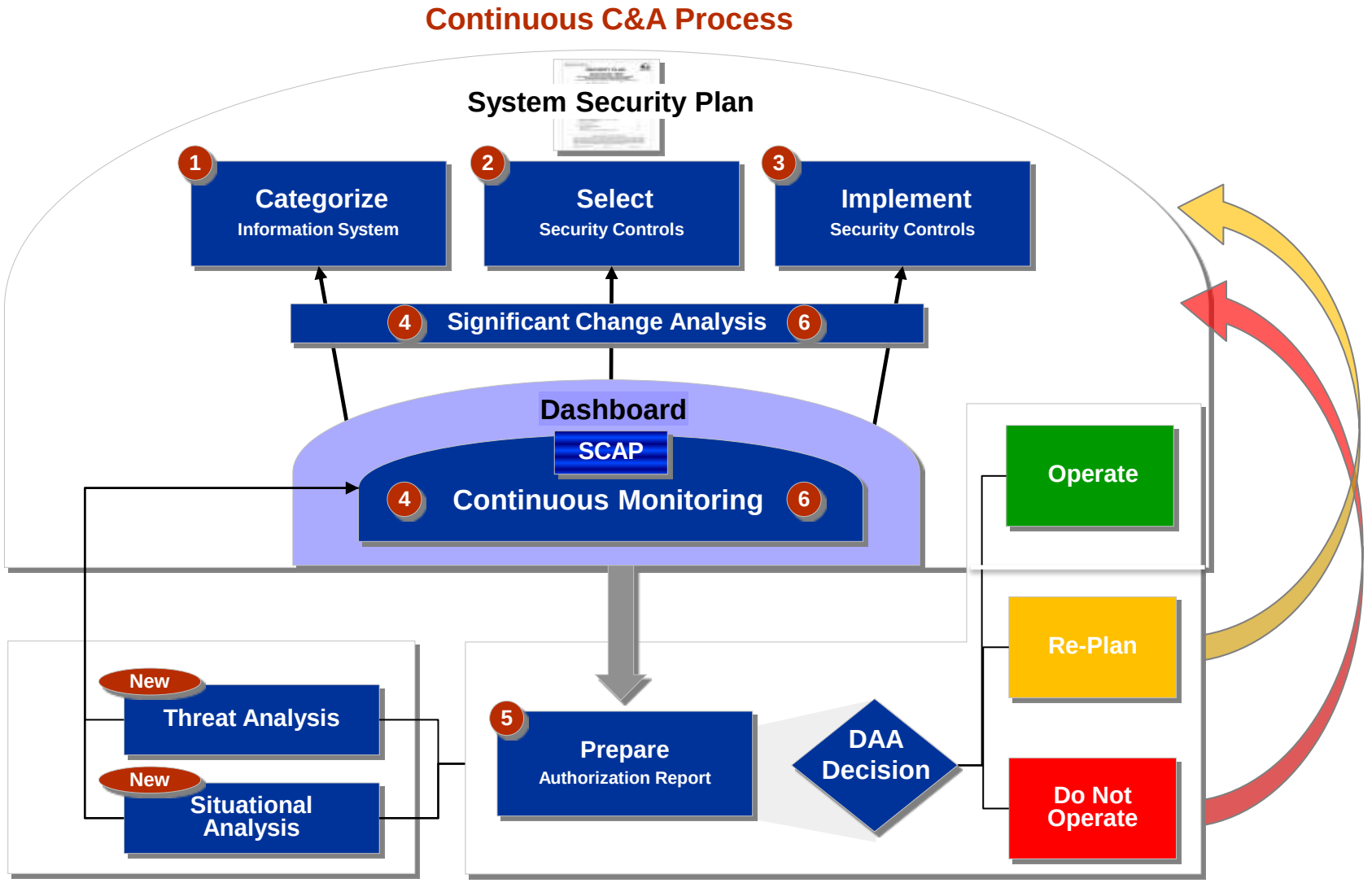
When the dashboard identifies new kinds of sensitive data in a system, that can immediately trigger re-categorization.

When the dashboard identifies new components (e.g., data base links not in the SSP) it can be used to trigger human authorization and SSP update, if appropriate.

The Security Plan informs the dashboard of what controls needs to be tested (These need to be recorded as SCAP tests).

When the dashboard identifies controls that need attention, it informs operators to change the implementation to make the controls work.

Continuous C&A Process will provide more effective real-time security – not just a snapshot in time

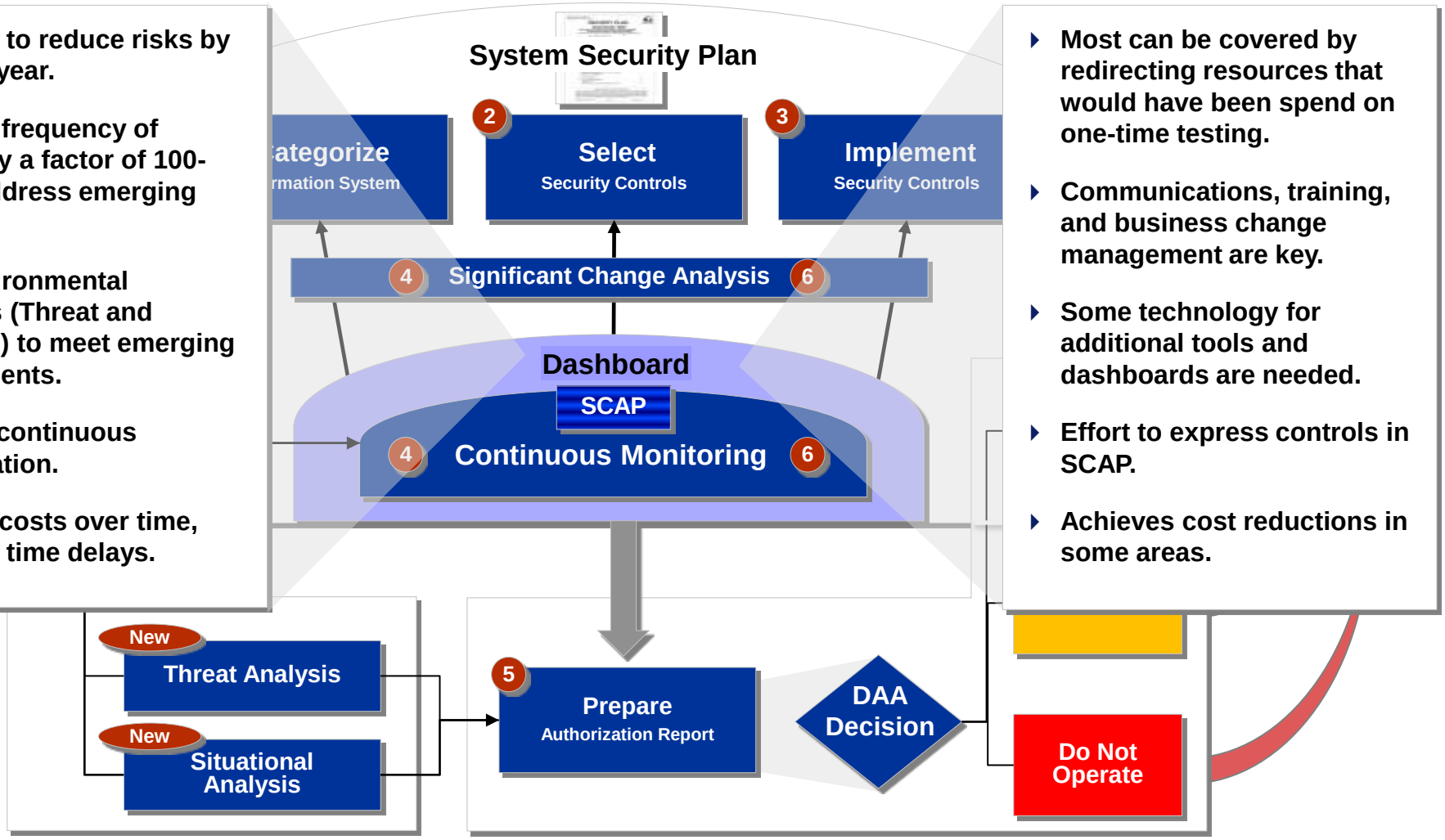


Although there is some cost inherent in the Continuous C&A process, its benefits are significant – and cannot be ignored

Benefits

- Potential to reduce risks by 90% per year.
- Increase frequency of testing by a factor of 100-300 to address emerging threats.
- Add Environmental Analyses (Threat and Situation) to meet emerging requirements.
- Enables continuous accreditation.
- Spreads costs over time, reducing time delays.

Continuous C&A Process

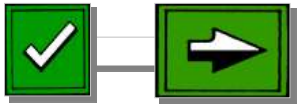


Costs

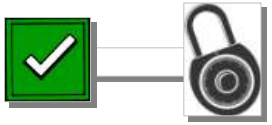
- Most can be covered by redirecting resources that would have been spend on one-time testing.
- Communications, training, and business change management are key.
- Some technology for additional tools and dashboards are needed.
- Effort to express controls in SCAP.
- Achieves cost reductions in some areas.

What Is Needed From SCAP?

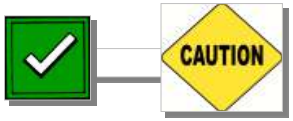
- A way to express everything that needs to be checked



- A way to express results that can be used to drive follow-on activities

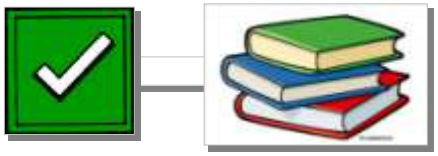


- A way to convert checks and results into a statement about controls



- A way to associate threat and impact to the checks and results

Issues and Opportunities



- A way to express everything that needs to be checked

NIST National Institute of Standards and Technology Information Technology Laboratory
Security Content Automation Protocol
SCAP

  - Community Content

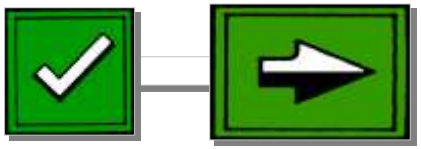
CPE
common platform enumeration

  - CPE

The·Open·Checklist·Interactive·Language·(OCIL)

  - OCIL

Issues and Opportunities



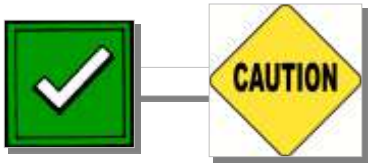
- A way to express results that can be used to drive follow-on activities
  - OVAL Results
  - Complex Checks
  - CCSS

The Common Configuration Scoring System (CCSS): Metrics for Software Security Configuration Vulnerabilities

Issues and Opportunities

- A way to convert checks and results into a statement about controls
  - CVE to Technical Control Mapping
  - CCE to Technical Control Mapping
  - Quality of Technical Control Assessment

Issues and Opportunities



- A way to associate threat and impact to the checks and results
  - CCE binning
  - Threat reporting

Questions

Contact Information

Kim Watson
Technical Director

NSA/IAD/VAO
9800 Savage Road
Ft Meade, MD 20755-6719
Tel (410) 854-7414
kkwatso@nsa.gov

Jim Ronayne
Systems Engineer
Varen Technologies

NSA/IAD/VAO
9800 Savage Road
Ft Meade, MD 20755-6719
Tel (410) 854-7585
jkronay@nsa.gov

George Moore
Chief Computer Scientist

Department of State, IRM/IA
1000 Wilson Blvd., Suite 1400
Arlington, VA 22209
Tel (703) 812-2203
mooregc@state.gov