IT Security Automation Conference 2011

Maximizing ROI for Continuous Monitoring

October 31, 2011
11:30 – 12:30
Arlington, VA

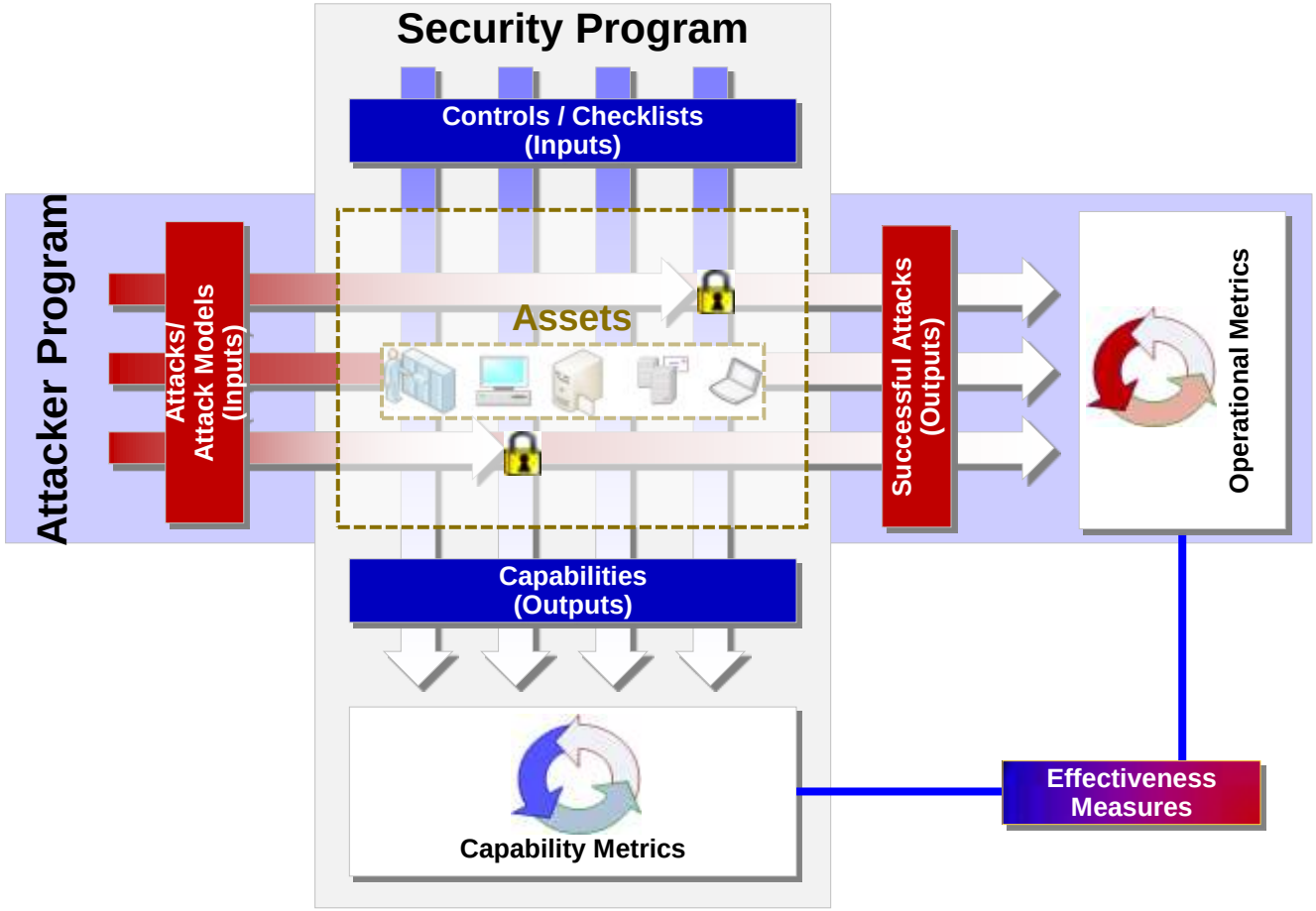
Agenda

Key Questions

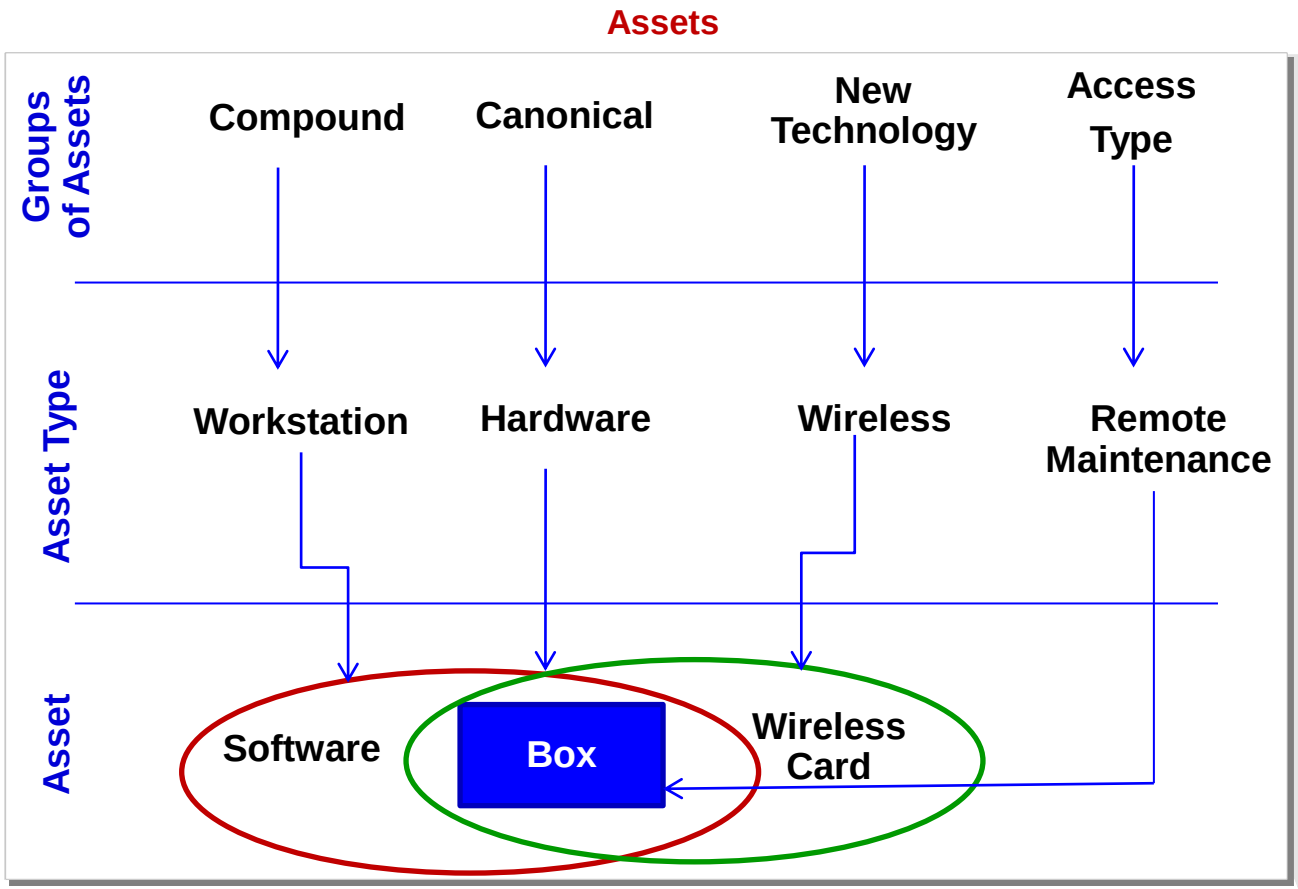
- Why do we need security programs?
- What should be protected?
- How are the assets protected?
- How do we know that they are protected well?
- How can we test and measure this protection efficiently?
- What are critical factors for success?

The ultimate purpose of security program is to effectively protect assets from attacks

Overview – Concept



Figuring out what to protect is not as straightforward



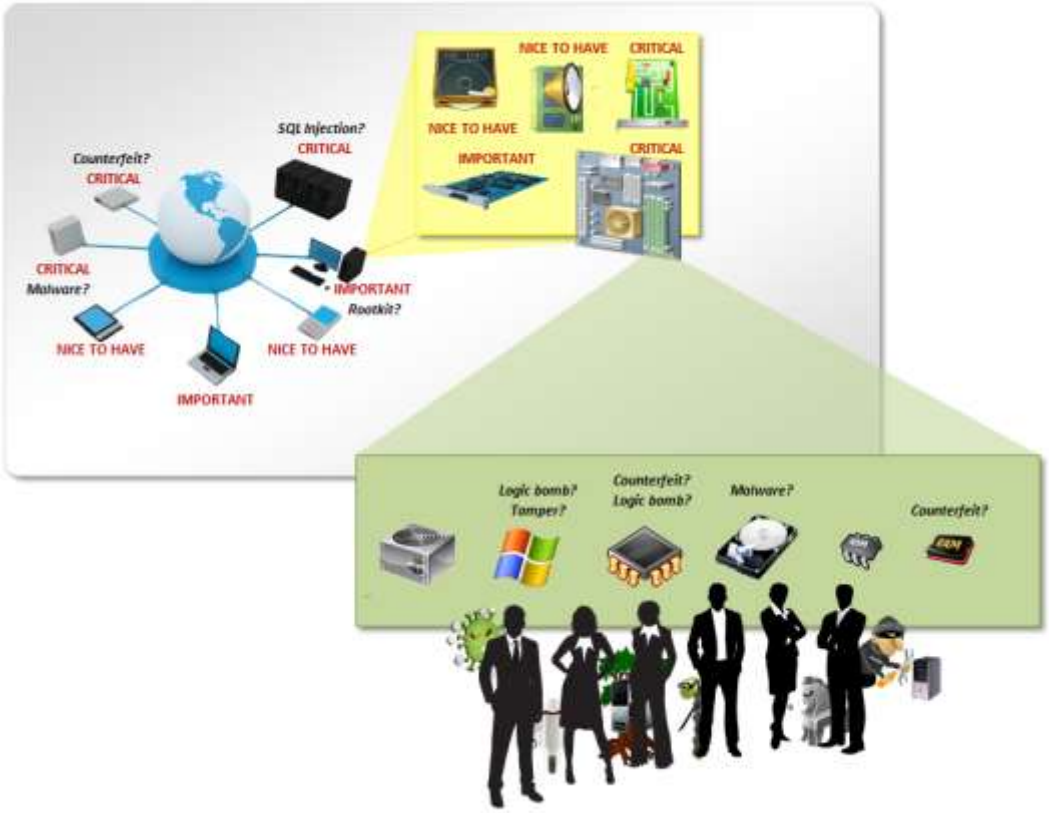
- **Canonical** – Mutually exclusive and exhaustive assets
  - Physical: Hardware, Facilities, Media
  - Information : Software, Data
  - Human : People
- **Compound – Commonly used groupings of assets that consist of some Canonical assets**
  - **Server**
  - **Workstation**
- **Technology – Compound assets that represent new or emerging technologies that require special security-related attention**
  - **Wireless**
  - **Cloud**
- **Ways of Accessing Assets –**
  - **Maintenance**
  - **Remote access**
  - **External parties**

We need to evolve our security programs to continually protect organization's assets…

Attack Possibilities

What commonalities exist?	▪ **83%** of victims were targets of opportunity ▪ **92% of attacks were not highly difficult** ▪ **86%** were discovered by a third party ▪ **96% of breaches were avoidable through simple or intermediate controls**
How do breaches occur?	▪ **50% utilized some form of hacking** ▪ 49% incorporated malware ▪ (lower percentages included physical attacks, privilege misuse, and social tactics)

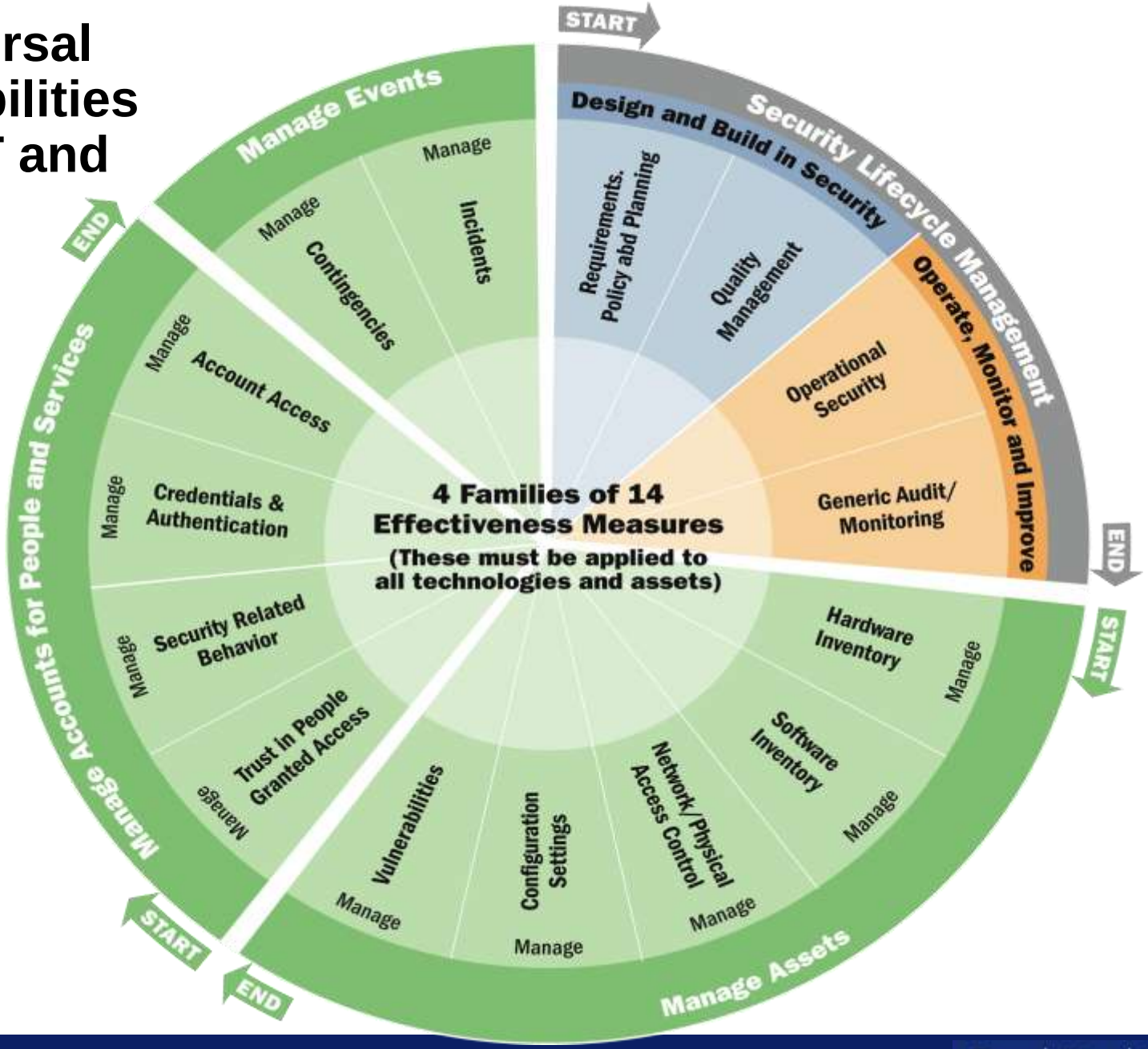
**** Source – 2011 Verizon Data Breach Investigations Report***



…however, historically, controls frameworks have not been structured for that purpose

We identified fourteen universal security capabilities based on NIST and CAG controls

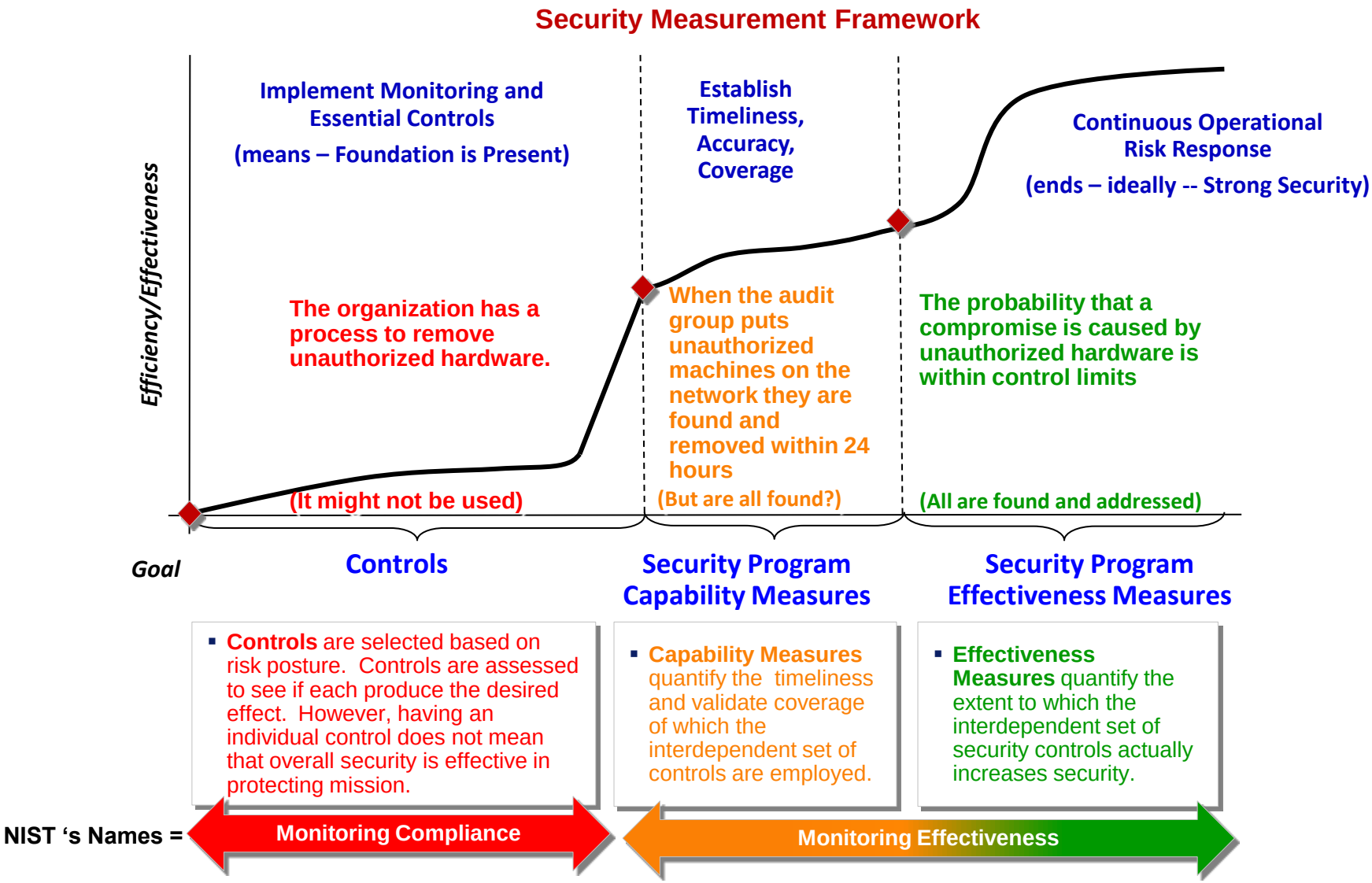
Notional Security Program



These security capabilities can cover all applicable assets

	Technologies and Assets											
4 Families of 14 Effectiveness Measures **(These must be applied to all technologies and assets)**	Networks	Applications	Data	People	Wireless	Cloud	Maintenance	Media	Physical	Environmenta.	Malware	Etc……
Security Lifecycle Management: Design and Build in Security *Requirement, Policy and Planning (L)* *Quality Management (G1)* Operate, Monitor and Improve *Operational Security (G2)* *Generic Audit/Monitoring (F)*												
Manage Hardware and Software Assets *Manage Hardware Inventory (A)* *Manage Software Inventory (B)* *Manage Network /Physical Access Control (C)* *Manage Configuration Settings (H)* *Manage Vulnerabilities (M)*												
Manage Accounts for People and Services *Manage Trust in People Granted Access (N)* *Manage Security Related Behavior (E)* *Manage Credentials & Authentication (J)* *Manage Account Access (D)*												
Manage Events *Manage Contingencies (I)* *Manage Incidents (K)*												

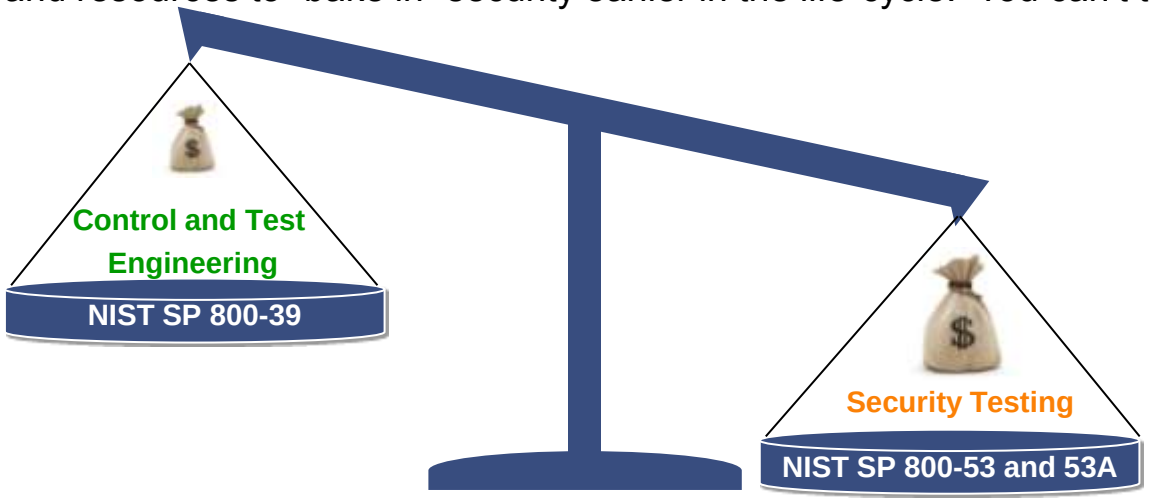
The community is moving towards an understanding that effectiveness of risk response is more valuable than compliance



Effectiveness measures that are based on NIST SP 800-53 controls and CAG could be used as measures for continuous monitoring

Benefits of Effectiveness Measures

- **Articulating effectiveness measures (called for in NIST 800-39) for NIST SP 800-53 control families provides significant benefits:**
  - **Providing Clearer Guidance** – If agencies understand the intent of systems of controls, they will better know how and when to select the appropriate types of controls based on the intended overall result.
  - **Avoiding Wasteful Testing** – If one tests the result, and finds that the whole system is working, we are measuring the "bottom line" of the system (i.e., It is cheaper to regularly test the bottom line than to test all the parts).
  - **Allows for more investment in Security Design (*By Reducing Cost of Security Testing*)** – Enables more time and resources to "bake in" security earlier in the life-cycle. You can't test in quality.



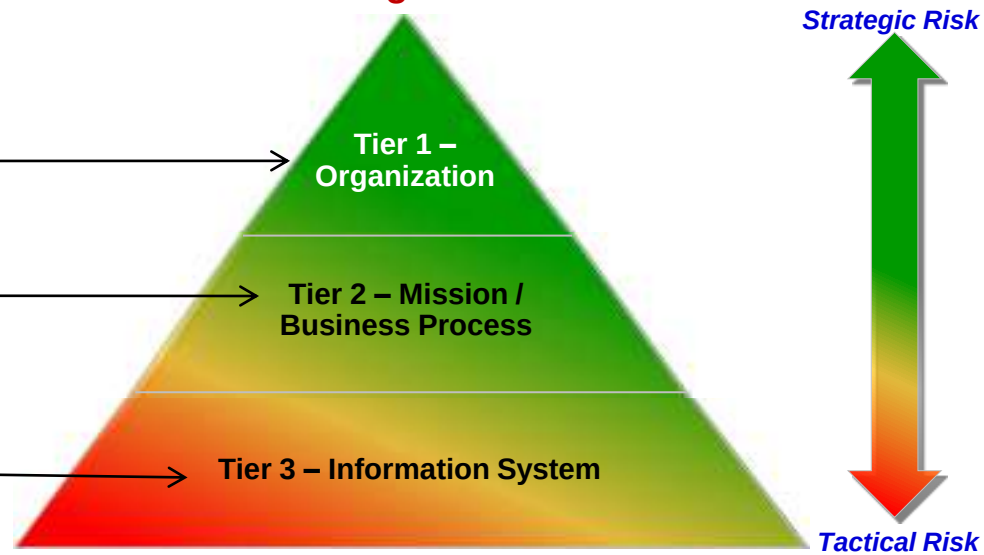
NIST 800-39 emphasized move to more engineering.

CAG emphasized avoiding testing with low ROI and using effectiveness measures

Recent NIST SP 800-39 guidance suggests that security testing should be prioritized based on a effectiveness of risk response

- According to 800-53, continuous monitoring activities align with the risk pyramid:
  - Traceable to organizational missions/business functions, federal legislation, directives, regulations, policies
  - Determine the ongoing effectiveness of risk response
  - Modify risk response based on effectiveness measures
  - Conduct assessment of the ongoing effectiveness of controls
  - Verify that planned risk response measures are implemented
  - Identify risk-impacting changes to organizational information systems and the environments in which the systems operate.

NIST SP 800-39
Risk Management Tiers



Measurement and testing higher on this hierarchy – especially measuring effectiveness of risk response – holds great promise.

Manual testing at the lowest level requires expensive testing.

ROI of testing is determined by…

Key Framework Definitions

1 Critical Control (Risk)*

Low Risk= Lower Frequency

- A control is **"critical"** to the extent that failure of the control itself increases risk (assuming other controls still work), where risk includes the vulnerability level created, the likely threats, and the impact of the possible resulting compromise. **In short, risk level (considering threat, vulnerability and impact) is a good measure of "criticality".**

NIST 800-53A & CAG

High Risk= Higher Frequency

2 Volatile Control (MTTF)*

Low MTTF= Higher Frequency

- A control is **"volatile" to the extent that its "mean time to failure (MTTF)" (or equivalent measure) is shorter**. Equivalent measures might include the probability distribution of failure, (better) median time to failure, or (best) time to X% probability of failure, where X% represents an acceptable level of risk.

NIST 800-53A

High MTTF= Lower Frequency

3 Marginal Cost of Testing**

Low Cost = Higher Frequency

- Where detailed testing of controls may be automated, such that the **marginal cost of testing** is sufficiently low, then testing should be nearly as frequent as practical, (e.g., hours to days). However, where the marginal cost of testing controls is high, justification exists for testing less frequently.

NIST 800-39 and CAG

High Cost = Lower Frequency

*The concepts of "critical" and "volatile" controls were introduced in NIST SP 800-53A.
The CAG also emphasized focusing testing on "where we are being attacked", i.e. high threat areas.

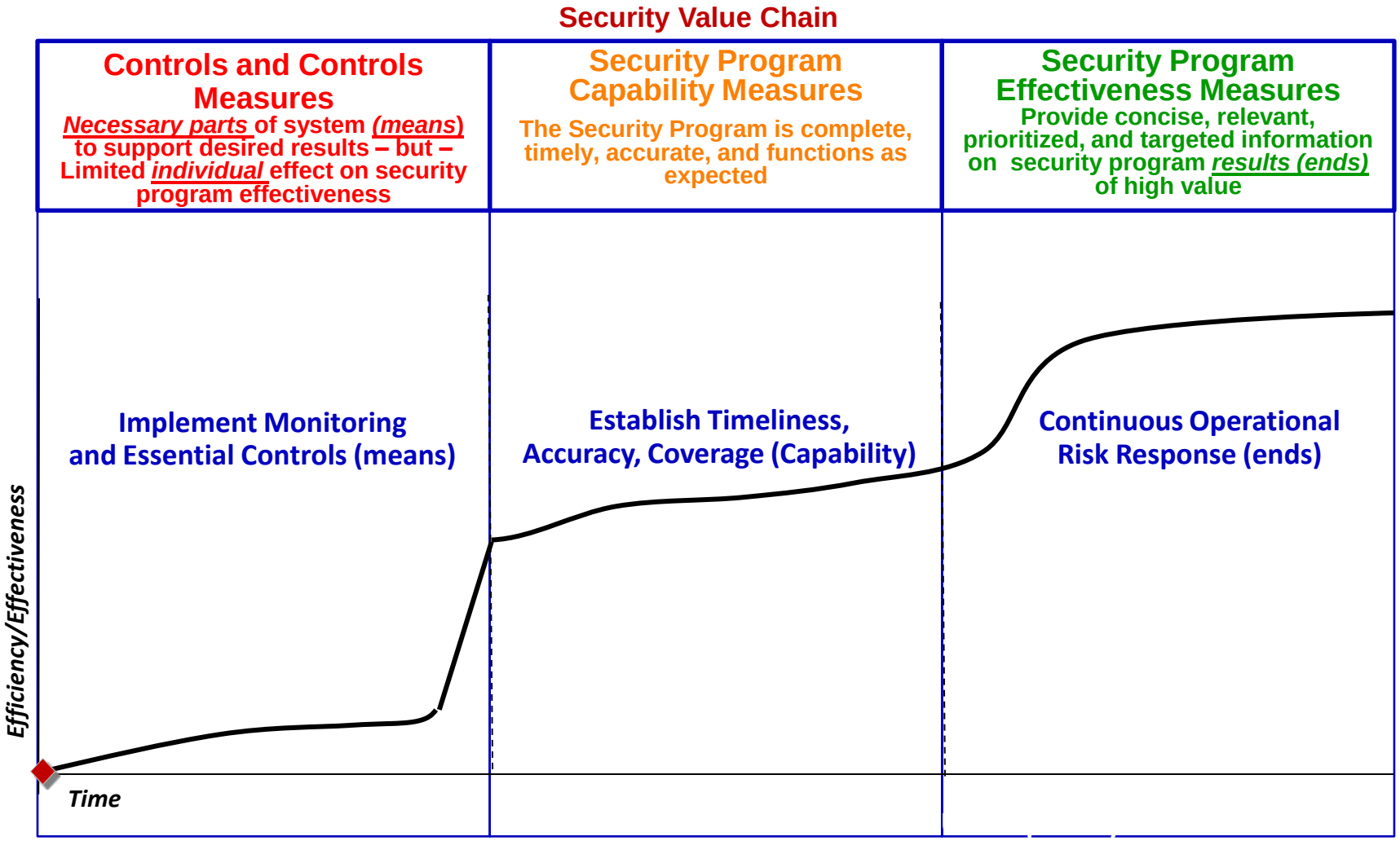
**The concept of "marginal cost of testing" was introduced in NIST SP 800-39.
The CAG also emphasized the need to manage the cost of testing.

Economic analysis validated frequent testing should be considered carefully

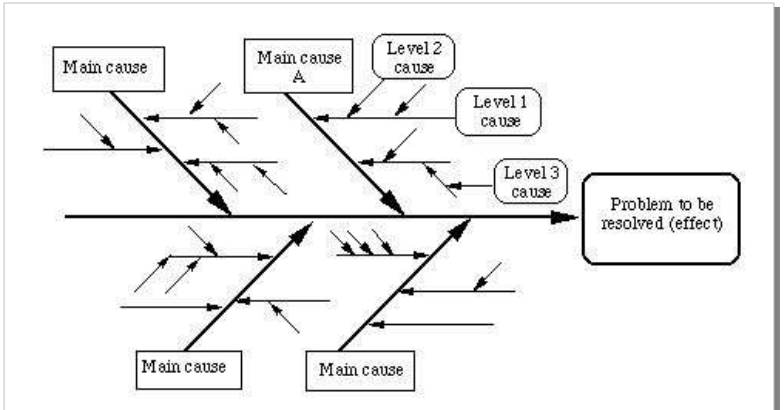
Frequency of Testing

1. **What to test Frequently?** -- Tests that can be done at very low marginal cost should be tested as frequently as possible (example -- vulnerability and configuration checks).
2. **What to test on an Event Driven basis?** -- Tests that cost more that 10% of the cost of failure should be tested on an event driven basis (when higher value outcomes indicate the need).
   - If in doubt about how frequently to test, it is better to err on the side LESS frequent testing than more.
3. **What not to Test? --** When the cost of testing is high enough (near the cost of a control failure, it is better not to test at all.
4. **What Effectiveness Measures to Test?** - A small set of high-value effectiveness measure should be identified and continuously monitored to identify when (and where) event driven testing is needed.
   - A set of 14 high value effectiveness measures have been identified which cover all of 800-53 and the CAG/CSC.
   - These are group into 4 broad families.
5. **More attention needs to be given to** finding the systemic source of detailed problems, rather than just fixing the symptoms. (More engineering relative to testing.)

Identifying controls effectiveness, capability, and program effectiveness measures is critical for defining a security value chain



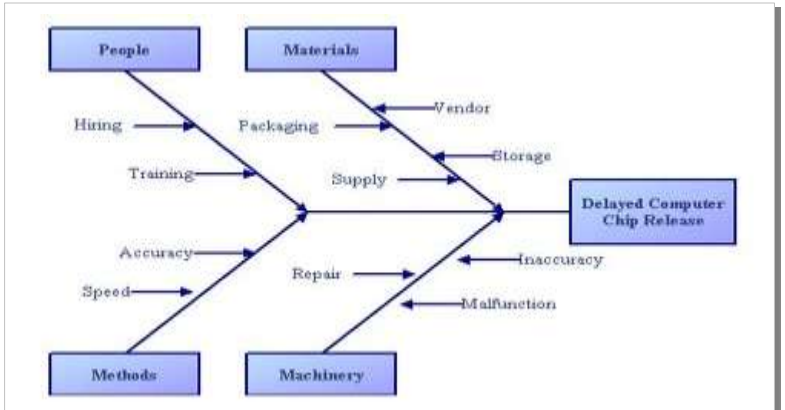
A powerful way to illustrate a security value chain is through the use of fish bone diagrams



http://pdca.wordpress.com/2006/05/09/ishikawa-fishbonecause-and-effect-diagram/

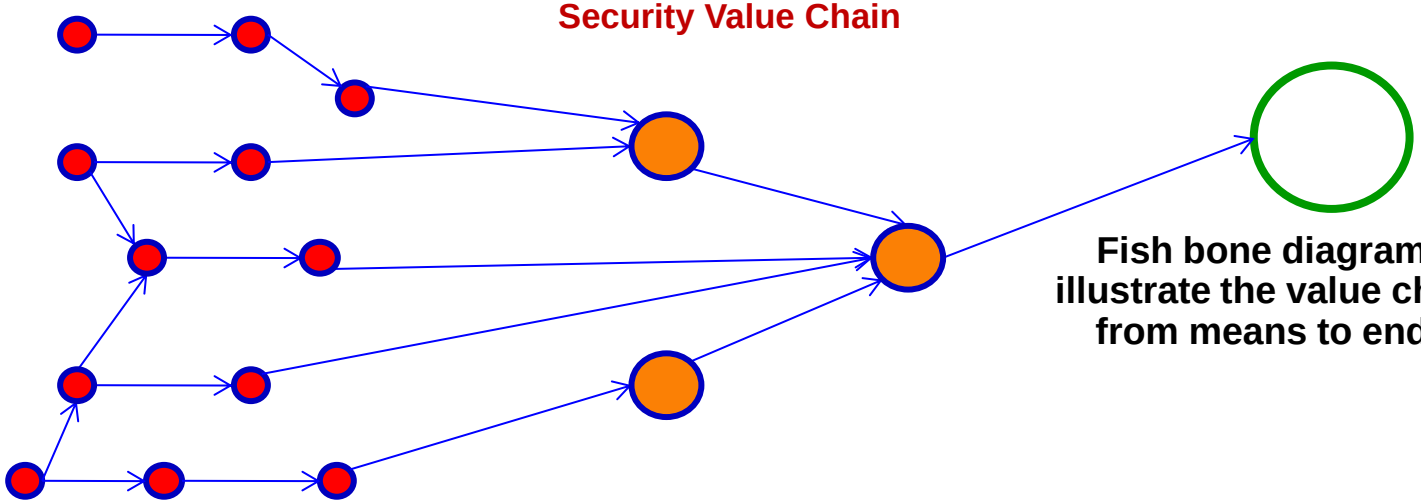
The Ishikawa diagram (also known as a Fishbone diagram) is a graphical method for finding the most likely causes for an undesired effect.

Kaoru Ishikawa, a famous Japanese consultant developed this method in the 1960s



http://technology.infomine.com/valueengineering/Value_files/image009.gif

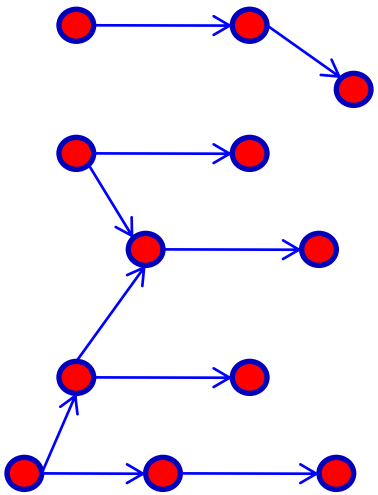
Security Value Chain



Fish bone diagrams illustrate the value chain from means to ends

The security value chain can be traced using a fish bone diagram comprised of the three types of measures

Security Value Chain

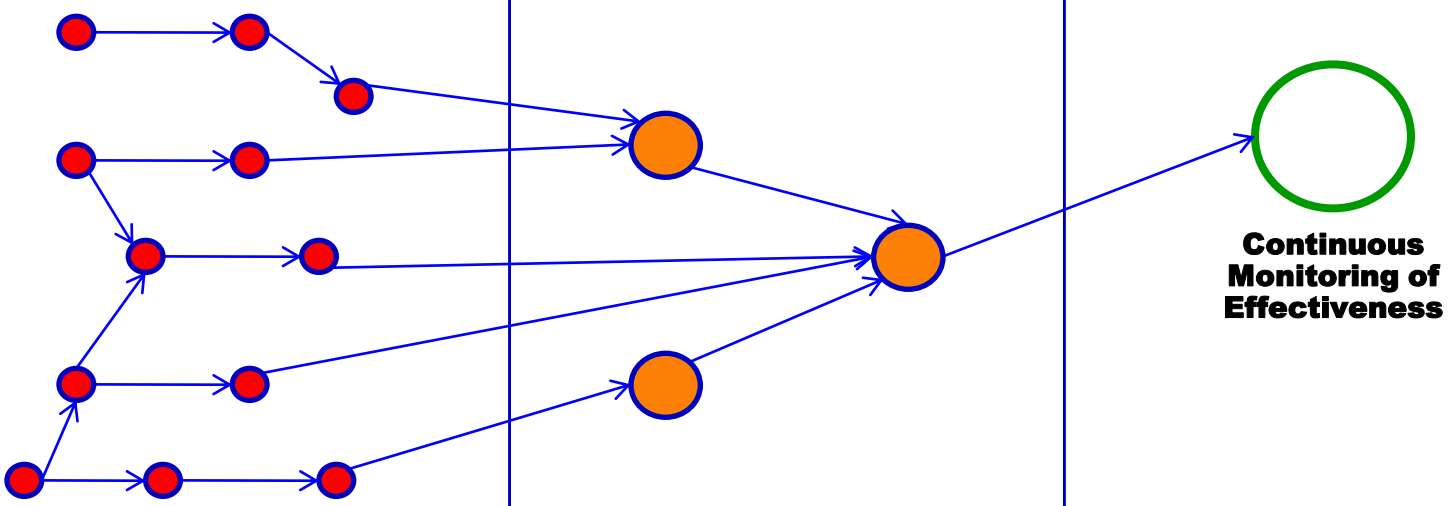
Controls and Controls Measures *Necessary parts* of system *(means)* to support desired results – but – Limited *individual* effect on security program effectiveness	Security Program Capability Measures The Security Program is complete, timely, accurate, and functions as expected	Security Program Effectiveness Measures Provide concise, relevant, prioritized, and targeted information on security program *results (ends)* of high value
800-53 Controls and 800-53A Tests	CAG Measures	800-39 Monitoring Effectiveness
 Under Traditional C&A we measure this, but don't know whether the result is good.		

= 800-53 Control

Building security value chain demonstrates role of individual controls in creating a holistic security program

Security Value Chain

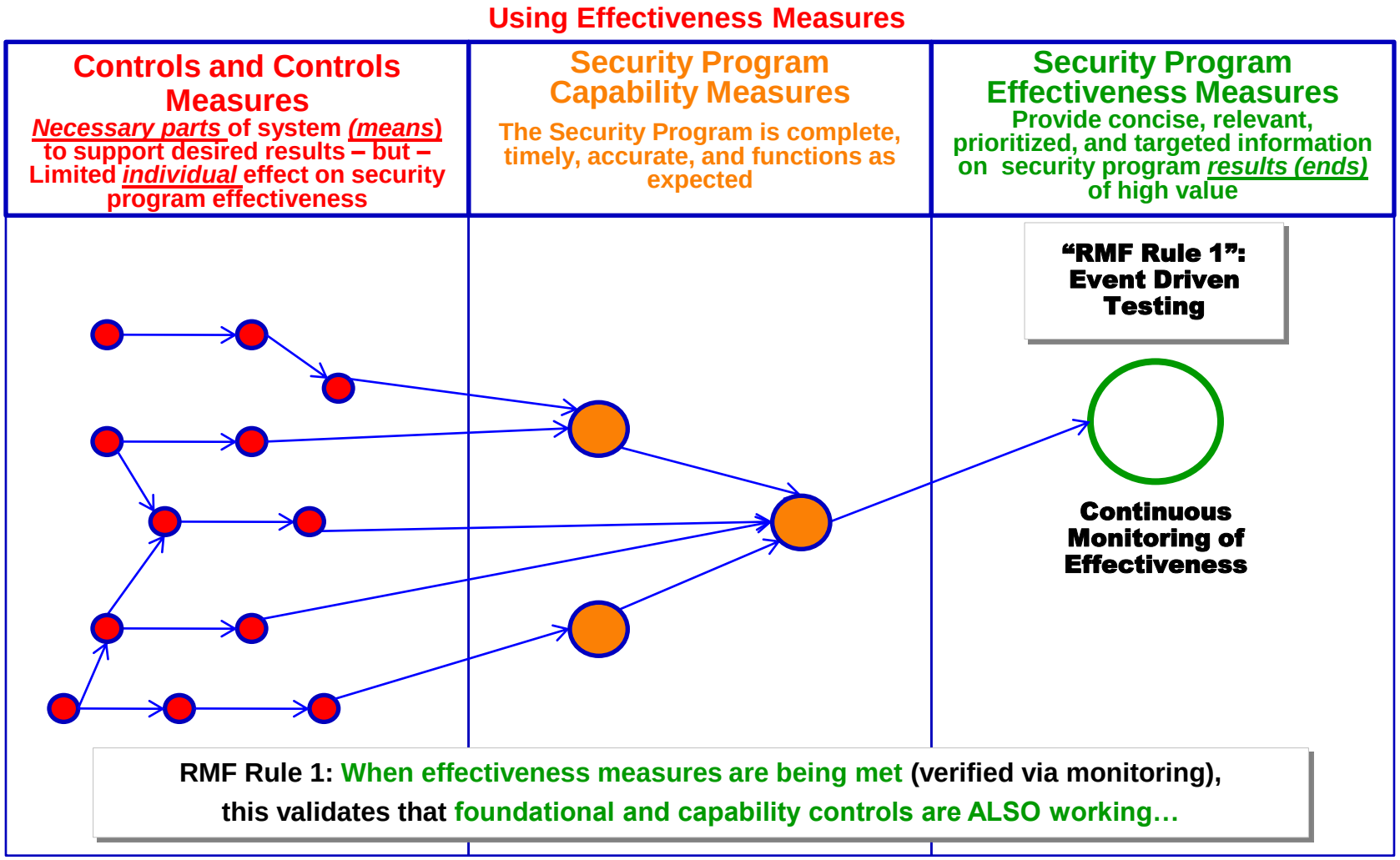
Controls and Controls Measures *Necessary parts* of system *(means)* to support desired results – but – Limited *individual* effect on security program effectiveness	Security Program Capability Measures The Security Program is complete, timely, accurate, and functions as expected	Security Program Effectiveness Measures Provide concise, relevant, prioritized, and targeted information on security program *results (ends)* of high value
800-53 Controls and 800-53A Tests	CAG Measures	800-39 Monitoring Effectiveness



Under Traditional C&A we measure this, but don't know whether the result is good.	Under traditional C&A we don't measure this. CAG emphasizes this.	Under traditional C&A we don't measure this. SP 800-39 emphasizes this

= 800-53 Control

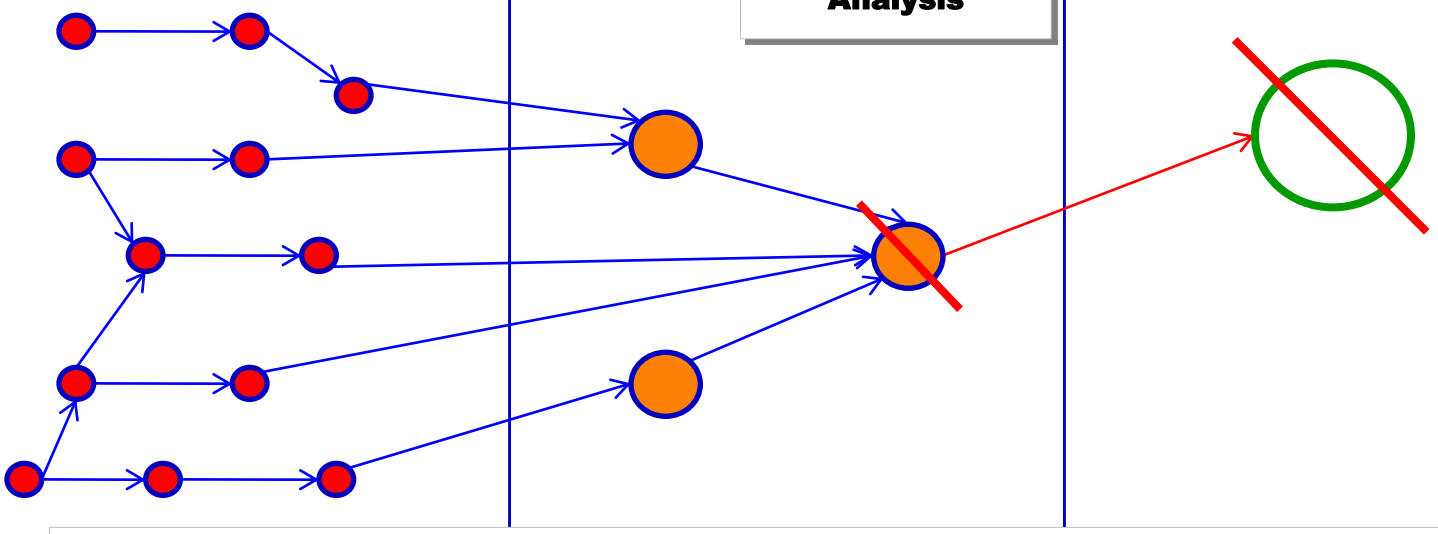
When effectiveness measures are not being met, it is not necessary to test all controls – because it is possible to trace back to the results



When effectiveness measures are not being met, it is not necessary to test all controls – because it is possible to trace back to the results

Using Effectiveness Measures

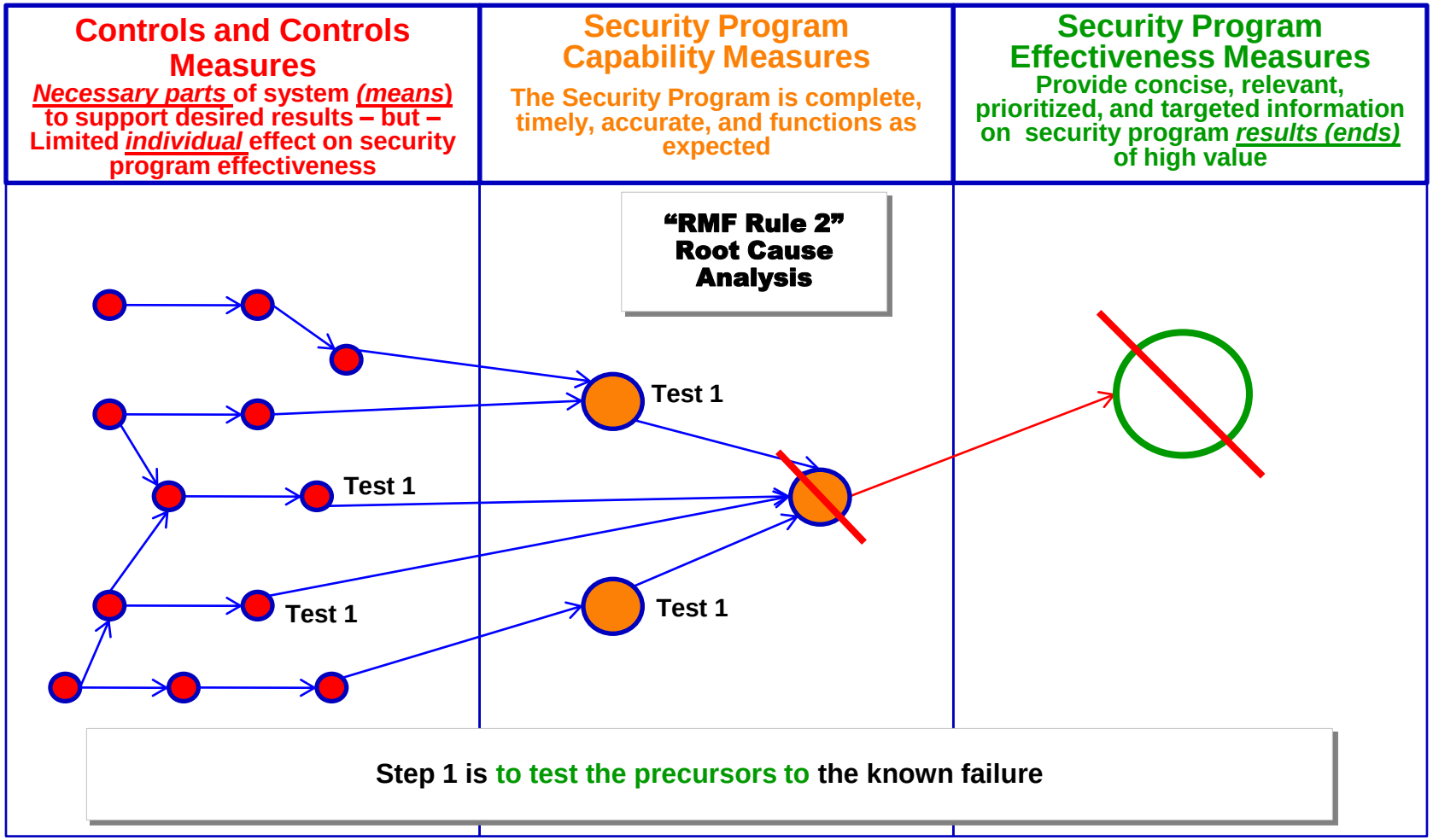
Controls and Controls Measures	Security Program Capability Measures	Security Program Effectiveness Measures
Necessary parts of system *(means)* to support desired results – but – Limited *individual* effect on security program effectiveness	The Security Program is complete, timely, accurate, and functions as expected	Provide concise, relevant, prioritized, and targeted information on security program *results (ends)* of high value



RMF Rule 2: When effectiveness measures fail we need to trace back to the cause, using the fishbone diagram

When effectiveness measures are not being met, it is not necessary to test all controls – because it is possible to trace back to the results

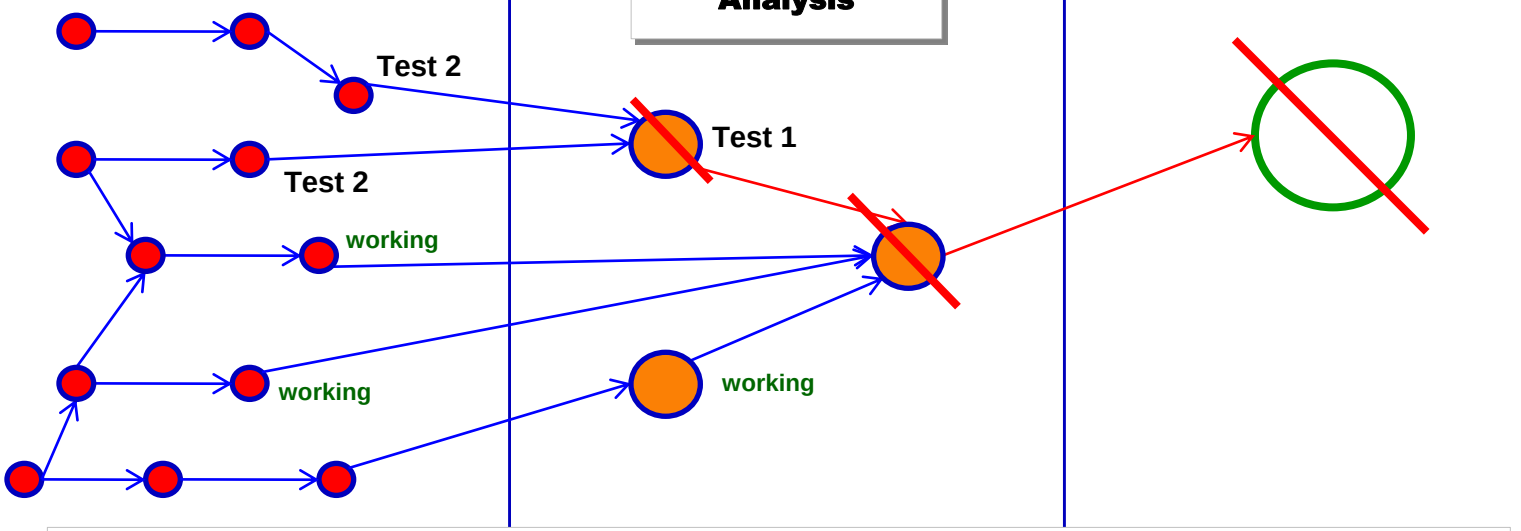
Using Effectiveness Measures



When effectiveness measures are not being met, it is not necessary to test all controls – because it is possible to trace back to the results

Using Effectiveness Measures

Controls and Controls Measures	Security Program Capability Measures	Security Program Effectiveness Measures
Necessary parts of system *(means)* to support desired results – but – Limited *individual* effect on security program effectiveness	The Security Program is complete, timely, accurate, and functions as expected	Provide concise, relevant, prioritized, and targeted information on security program *results (ends)* of high value

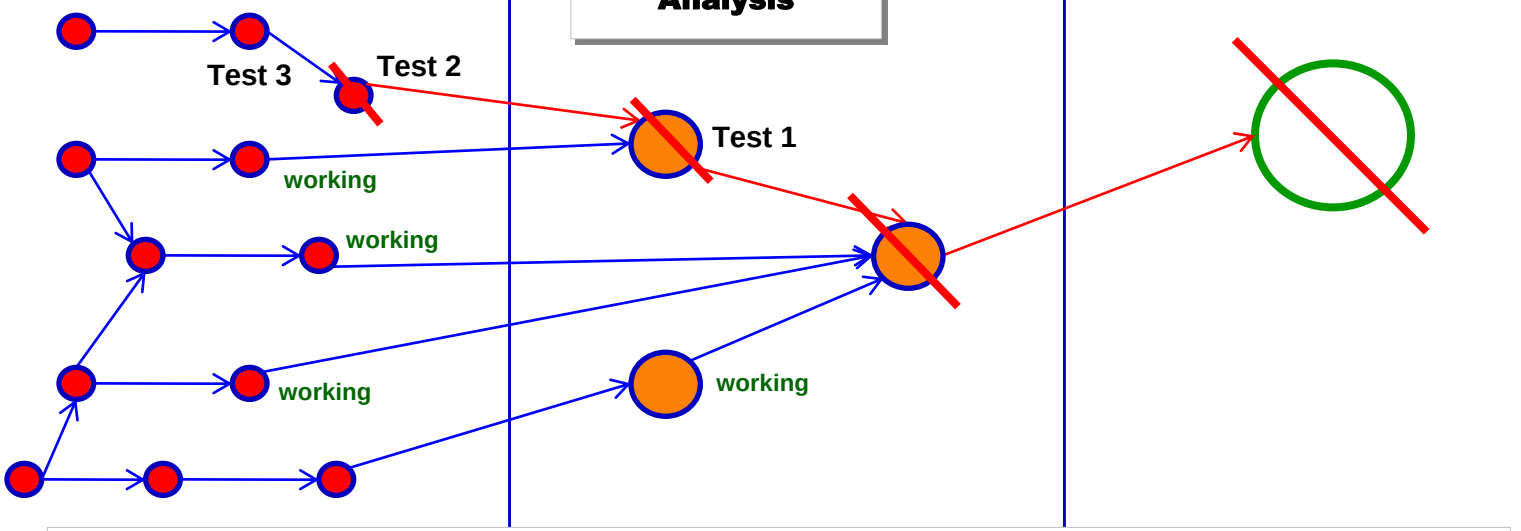


Step 2 is to trace back to the precursor of the new items that failed

When effectiveness measures are not being met, it is not necessary to test all controls – because it is possible to trace back to the results

Using Effectiveness Measures

Controls and Controls Measures	Security Program Capability Measures	Security Program Effectiveness Measures
Necessary parts of system *(means)* to support desired results – but – Limited *individual* effect on security program effectiveness	The Security Program is complete, timely, accurate, and functions as expected	Provide concise, relevant, prioritized, and targeted information on security program *results (ends)* of high value

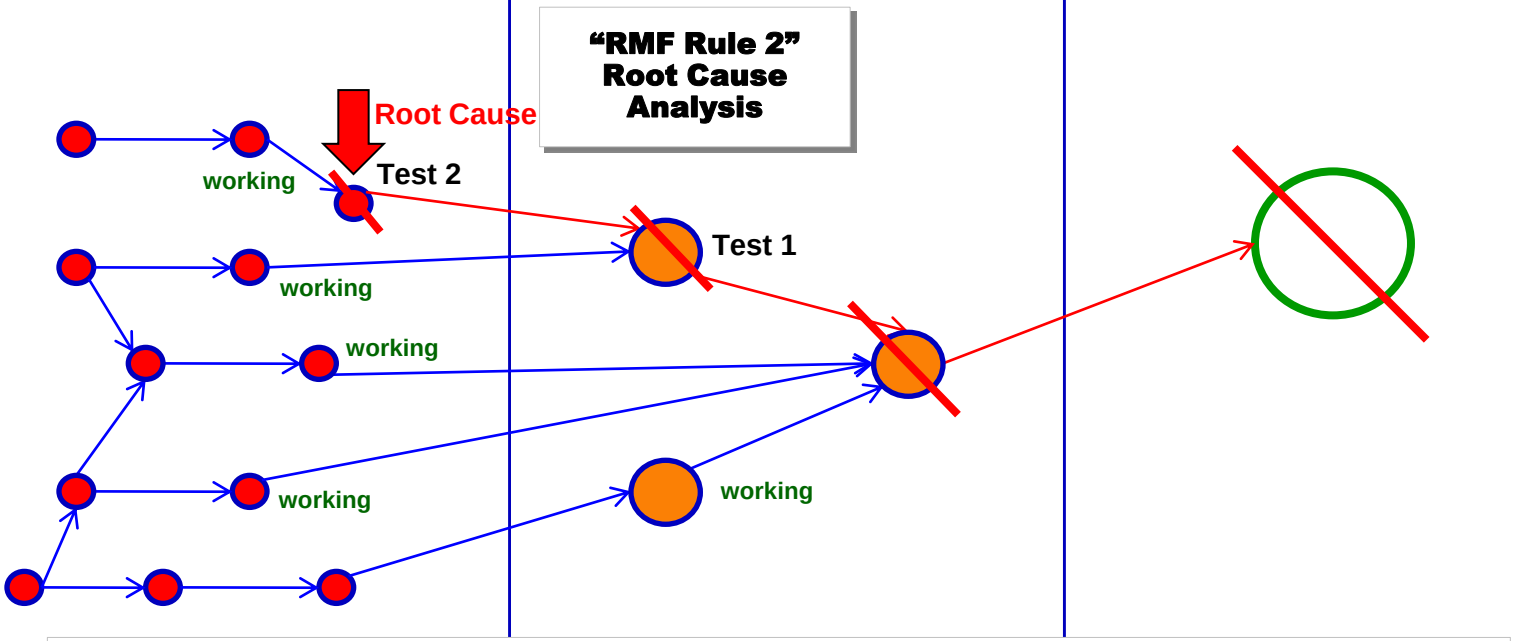


Step 3 is to trace back to the precursor of the Test 2 items that failed

When effectiveness measures are not being met, it is not necessary to test all controls – because it is possible to trace back to the results

Using Effectiveness Measures

Controls and Controls Measures	Security Program Capability Measures	Security Program Effectiveness Measures
Necessary parts of system *(means)* to support desired results – but – Limited *individual* effect on security program effectiveness	The Security Program is complete, timely, accurate, and functions as expected	Provide concise, relevant, prioritized, and targeted information on security program *results (ends)* of high value

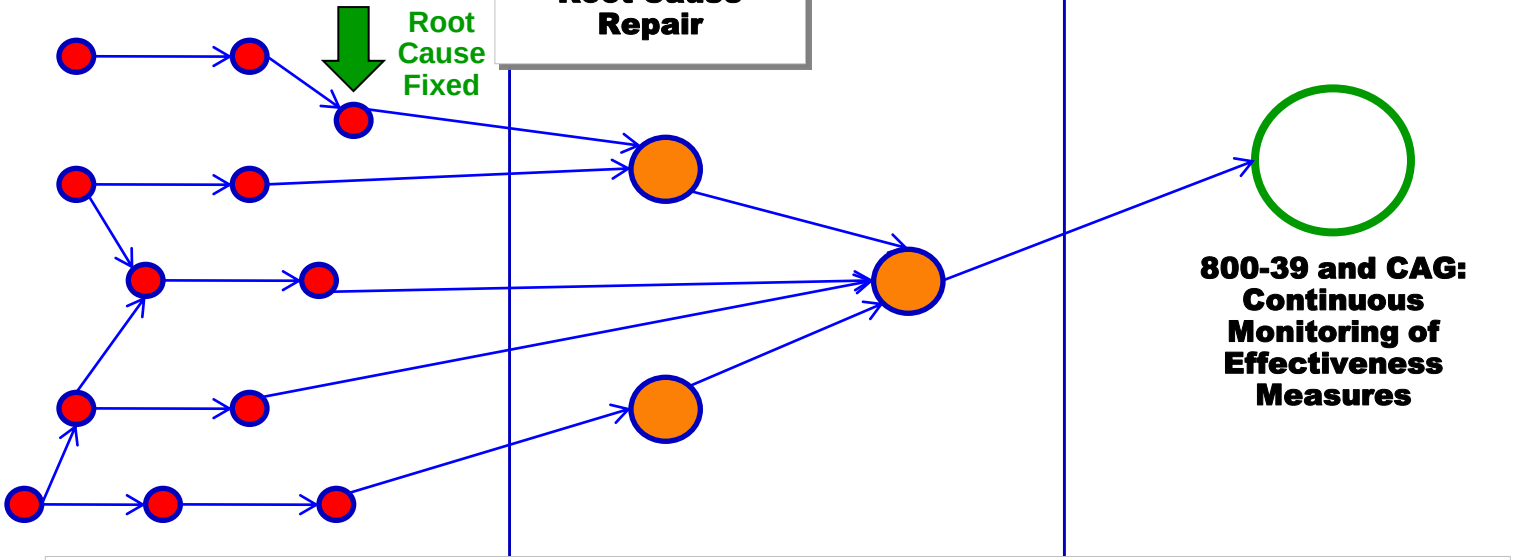


In this case, Test 3 shows that the item that failed in Test 2 is the root cause of the problem.
Not all items had to be tested, and they were only tested when needed – saving resources

When the root cause is found, the problem can be fixed

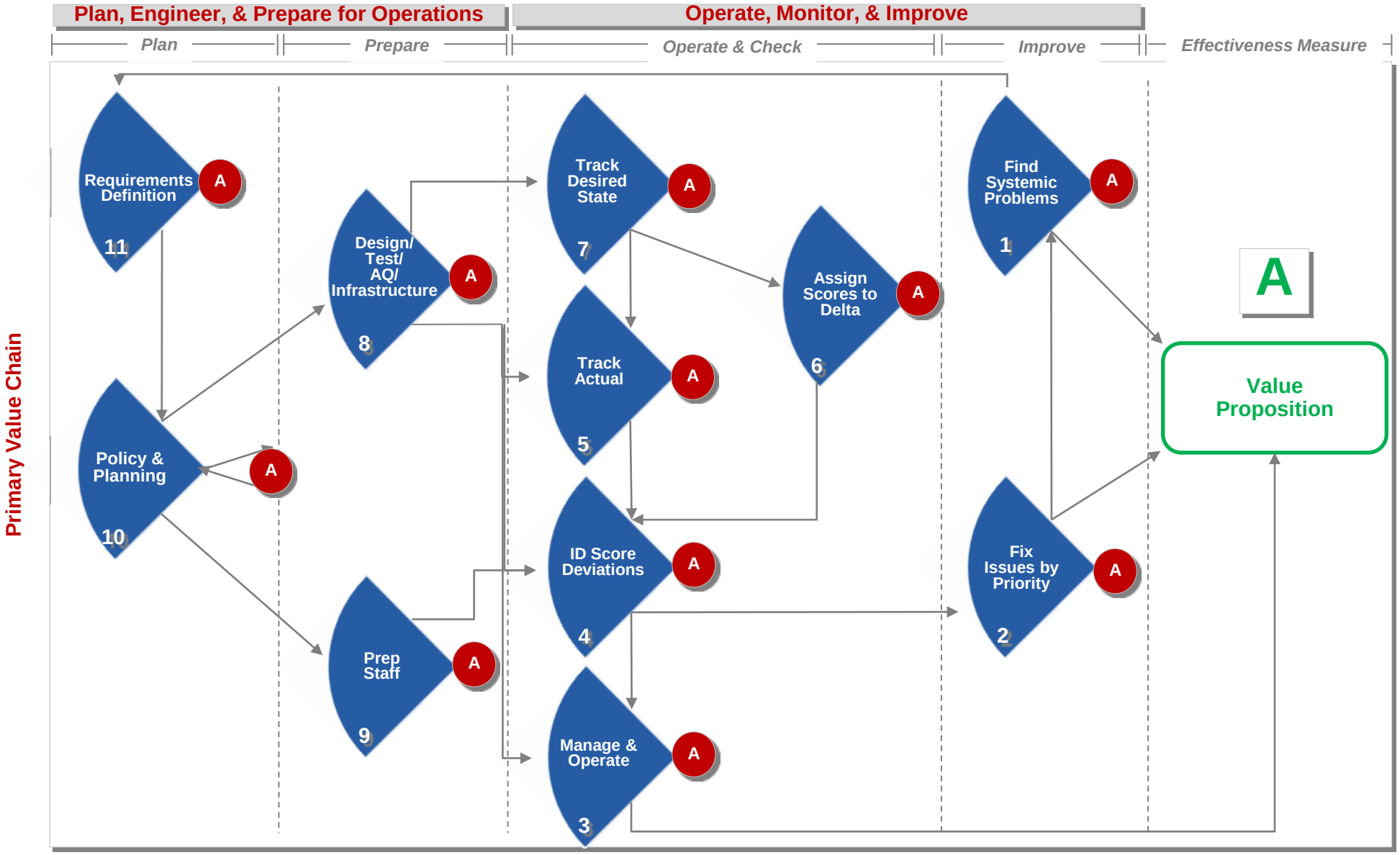
Using Effectiveness Measures

Controls and Controls Measures	Security Program Capability Measures	Security Program Effectiveness Measures
Necessary parts of system *(means)* to support desired results – but – Limited *individual* effect on security program effectiveness	The Security Program is complete, timely, accurate, and functions as expected	Provide concise, relevant, prioritized, and targeted information on security program *results (ends)* of high value



After fixing the root cause, the system works again.
This strategy reduces testing costs for expensive tests.

The generic Value Chain is based on NIST controls and spans the entire lifecycle from requirements to operations and improvement



Conclusion

- NIST controls grew organically over the last 10 years before the Internet was ubiquitous
- These controls and the manual ways of testing no longer scale for the current technology and threat environment
- A new approach is needed to test and measure effectiveness in real time while decreasing lifecycle costs and continually protecting assets against the evolving threat
- Long term commitment is required for success

- **Booz Allen and Department of State created a new way of solving this problem**
  - Not all controls are created equal, some need to be tested more frequently then others
  - Testing needs to revolve around effectiveness measures
  - Testing effectiveness measures creates efficiency and cost savings

- We need to help build momentum in the community to adopt and improve this methodology

Questions…

Contact Information

Nadya Bartol
Senior Associate

Booz | Allen | Hamilton

Booz Allen Hamilton, Inc.
One Preserve Parkway
Rockville, MD 20852, USA
Tel (301) 444-4114
Cell (301) 922-9537
Bartol_Nadya@bah.com

Jamie Miller
Senior Associate

Booz | Allen | Hamilton

Booz Allen Hamilton, Inc.
8283 Greensboro Drive
McLean, VA 22102, USA
Tel (703) 377-1274
Cell (202) 390-8919
Miller_Jamie@bah.com