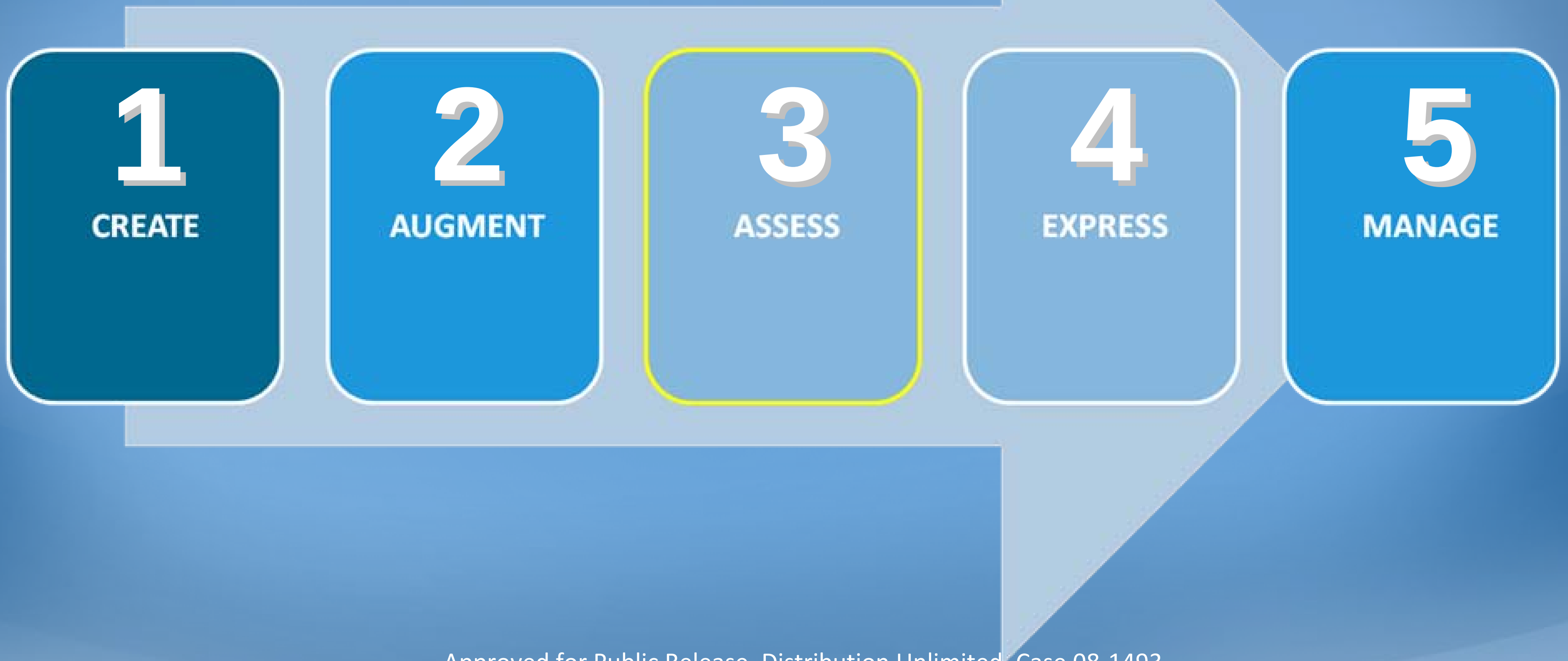
Phase 3: Automating Assessment

OVAL, OCIL, and writing compliance checks



1 CREATE

2 AUGMENT

3 ASSESS

4 EXPRESS

5 MANAGE

Approved for Public Release. Distribution Unlimited. Case 08-1493

Automating Compliance Assessment

- Create checks used to determine compliance with a desired state (recommendation)
- Use a standardized format to ensure guidance is easily consumed by a broad audience and range of tools
- Checking systems:
  - OVAL – System configuration checking (check category)
  - OCIL – End user questions (question category)

What is OVAL?

- Open Vulnerability and Assessment Language
- XML-based framework for describing and testing for machine states
- Can describe many different machine states
  - Vulnerable
  - Compliant
  - Installed application
  - Patch required
- A community-developed, international open standard

http://oval.mitre.org/

What is OCIL?

- Open Checklist Interactive Language
- XML-based framework for expressing compliance questionnaires
- Supports questions and follow up questions
- Defines logical constructs to allow lengthy questionnaires to be evaluated and produce a single result
- An emerging specification

http://nvd.nist.gov/ocil.cfm

Investigate

Discover Controls for Configuration Settings

Configuration Setting Discovery

Discover Controls for Configuration Settings

Recommendation: Require CTRL+ALT+DEL for login.

How-To: GUI path to put the configuration in place.

Where can I find the low-level settings that indicate that the system is configured properly?

Need to gather data required for a compliance check.

✓ **Compliant**

✗ **Not compliant**

Configuration Setting Discovery

Discover Controls for Configuration Settings

Recommendation: Require CTRL+ALT+DEL for login.

It is a registry key!!!

HIVE = HKEY_LOCAL_MACHINE
KEY = Software\Microsoft\Windows\CurrentVersion\Policies\System
NAME = disablecad
VALUE = ???

✓ **Compliant means value = 0**

✗ **Not compliant means value != 0**

Discovery Challenges

- Manual search very difficult, cumbersome
  - Digging into Active Directory, the Registry, the Metabase, configuration files, variety of repositories, etc.
- Most data repositories are huge
- There is seldom useful documentation
  - Even when documented, documentation seldom goes into the necessary detail

The Tools We Used to Find this Data

- ADSIEdit for searching Active Directory
  - Allows you to browse Active Directory
- Process Monitor for searching the Registry and filesystem
  - Allows browsing, editing, and monitoring
- wbemtest for exploring the WMI interface
  - Allows browsing of namespaces and objects
- All of the above are for Windows. Different tools are needed on other operating systems
- Tool utility varies
  - Some tools just show the current values
  - Some tools can take snapshots and note changes in a repository

Windows Investigator Tool (WIT)

- Developed by MITRE; provided on class CD
- Provides browsing, searching, scanning, and monitoring
  - Windows Management Instrumentation (WMI) & Active Directory
- Provides a means for authors of security benchmarks to map high-level actions to changes in low-level repositories
- Easily extensible for new repositories

Demo: Windows Investigator Tool

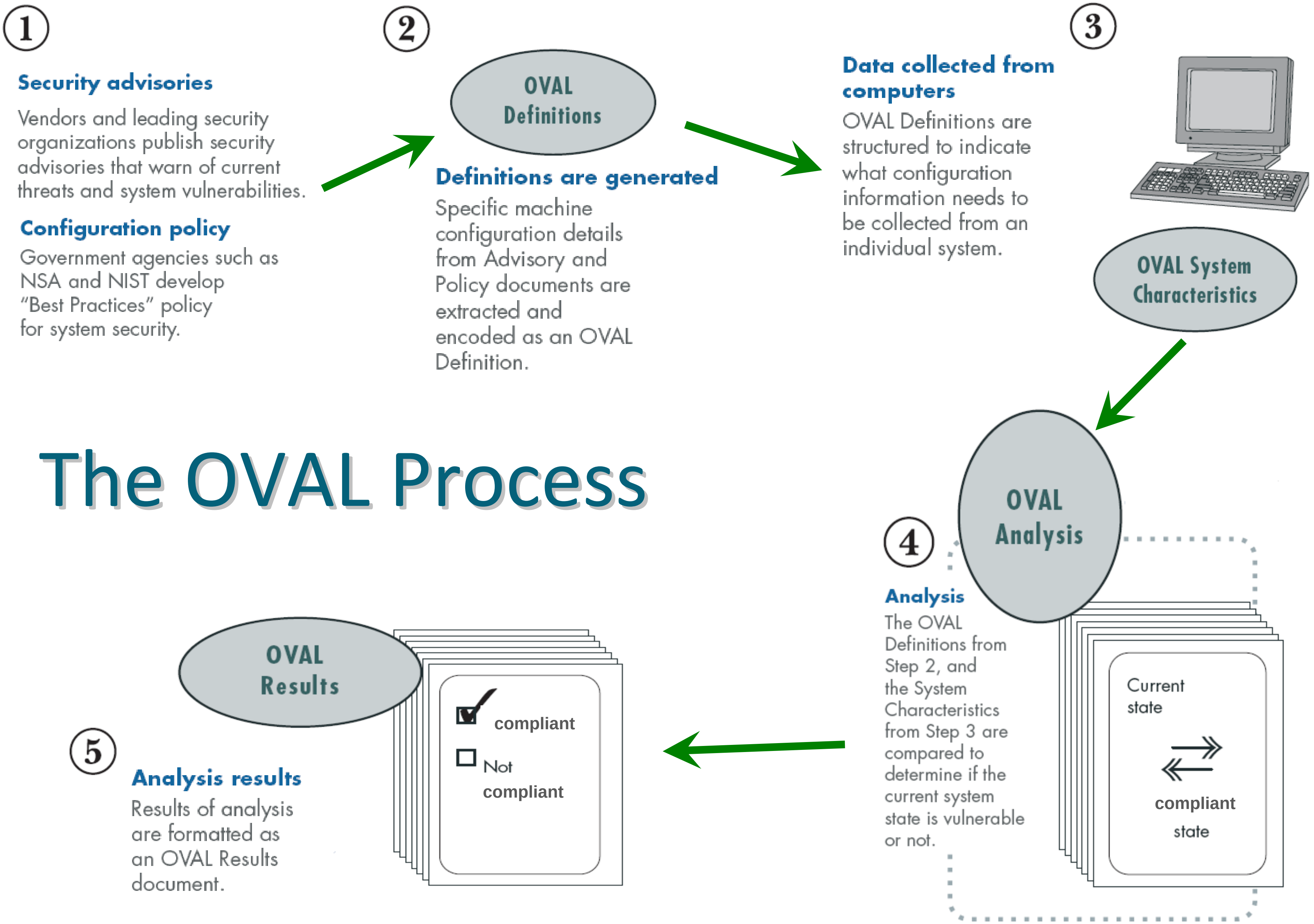
Introduction to OVAL

What is OVAL?

- Open Vulnerability and Assessment Language
- XML-based framework for describing and testing for machine states
- Can describe many different machine states
  - Vulnerable
  - Compliant
  - Installed application
  - Patch required
- A community-developed, international open standard

http://oval.mitre.org/

The OVAL Process



1

Security advisories

Vendors and leading security organizations publish security advisories that warn of current threats and system vulnerabilities.

Configuration policy

Government agencies such as NSA and NIST develop "Best Practices" policy for system security.

2

OVAL Definitions

Definitions are generated

Specific machine configuration details from Advisory and Policy documents are extracted and encoded as an OVAL Definition.

3

Data collected from computers

OVAL Definitions are structured to indicate what configuration information needs to be collected from an individual system.

OVAL System Characteristics

4

OVAL Analysis

Analysis

The OVAL Definitions from Step 2, and the System Characteristics from Step 3 are compared to determine if the current system state is vulnerable or not.

Current state

compliant state

5

OVAL Results

Analysis results

Results of analysis are formatted as an OVAL Results document.

☑ compliant

□ Not compliant

OVAL Language: Key Pieces

OVAL Definitions Schema

- Framework for logical assertions about a system
- Used to automate “check” rules in benchmarks

OVAL System Characteristics Schema

- Encoding of the details of a system (database of system info)
- Used silently in automated benchmarks

OVAL Results Schema

- Encoding of the detailed results of an analysis
- Used silently to pass OVAL return values to benchmark processor

http://oval.mitre.org/language/

OVAL Interpreter

- Freely available reference implementation
- Demonstrates usability of the OVAL Language
- Helps drive the development of the OVAL Language
- Validate & test content
- A reference for developers
- Reduces the cost of OVAL adoption

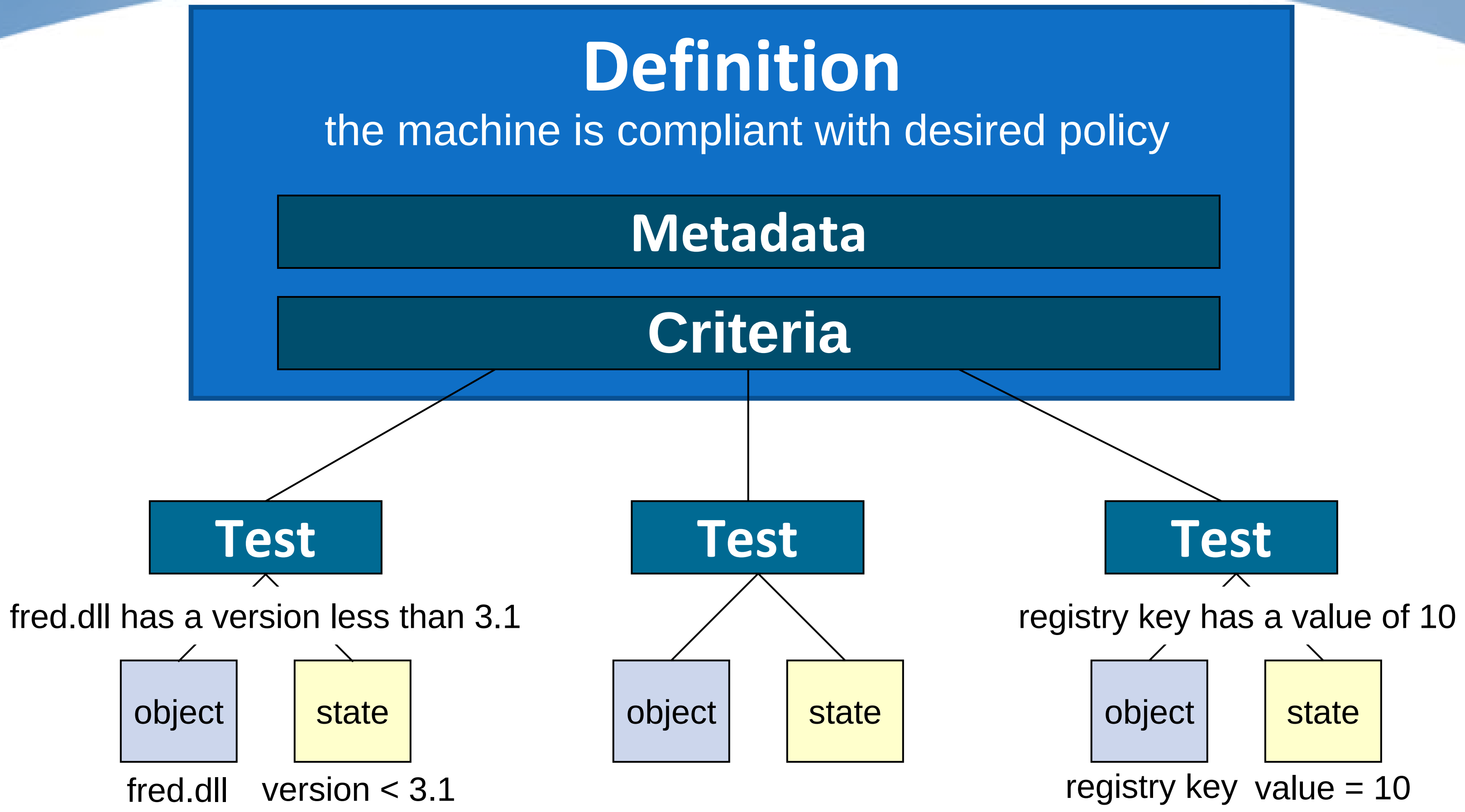
http://oval.mitre.org/language/download/interpreter

Demo: OVAL Process

Assessing your local system

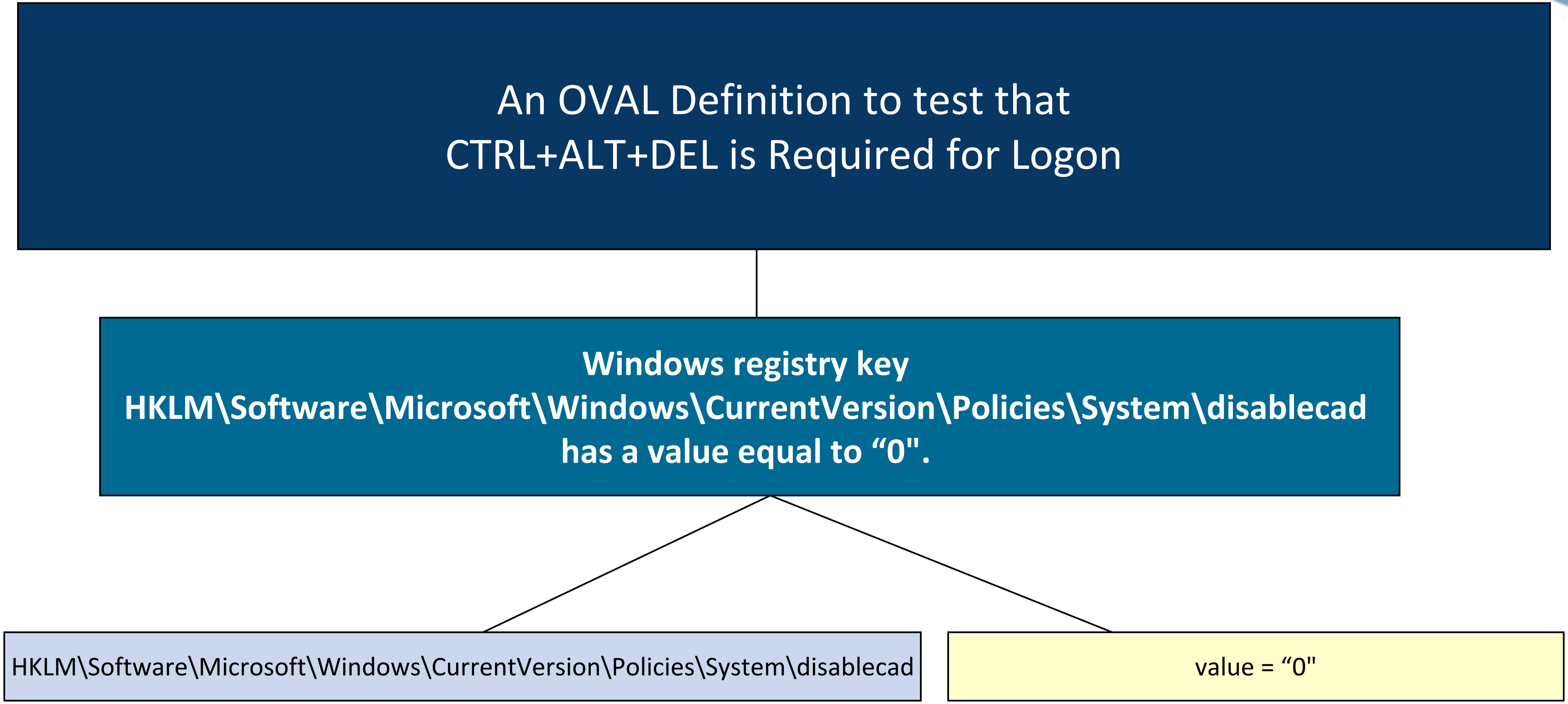
OVAL Definition Tutorial

Structure of an OVAL Definition



MITRE

CTRL+ALT+DEL - OVAL Definition



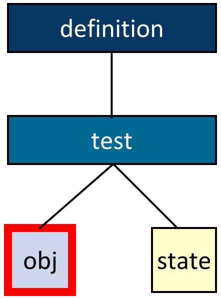
An OVAL Definition to test that
CTRL+ALT+DEL is Required for Logon

Windows registry key
HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\disablecad
has a value equal to “0".

HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\disablecad

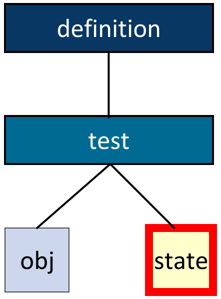
value = “0"

CTRL+ALT+DEL - Registry Object



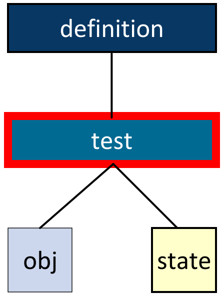
```
<registry_object id="oval:com.example:obj:1">
   <hive>HKEY_LOCAL_MACHINE</hive>
   <key>Software\Microsoft\Windows\CurrentVersion\Policies\System</key>
   <name>disablecad</name>
</registry_object>
```

CTRL+ALT+DEL - Registry State



```
<registry_state id="oval:com.example:ste:1">
  <value datatype="int" operation="equals">0</value>
</registry_state>
```

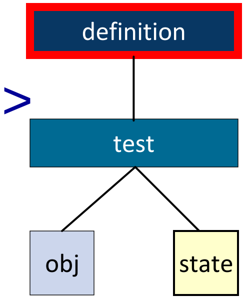
CTRL+ALT+DEL - Registry Test



```
<registry_test id="oval:com.example:tst:1" check="all">
    <object object_ref="oval:com.example:obj:1"/>
    <state state_ref="oval:com.example:ste:1"/>
</registry_test>
```

CTRL+ALT+DEL - OVAL Definition

```
<definition id="oval:com.example:def:1">
  <metadata>
    <title>CTRL+ALT+DEL Required for Logon</title>
    <description>
      This definition is used to introduce the
      OVAL Language to individuals interested
      in writing OVAL Content.
    </description>
  </metadata>
  <criteria>
    <criterion test_ref="oval:com.example:tst:1"
   comment="The registry key is set to require
   CTRL+ALT+DEL for Logon"/>
  </criteria>
</definition>
```



```xml
<oval_definitions …>
 <generator>…</generator>
 <definitions>
  <definition id="oval:org.mitre.oval.tutorial:def:1" version="1" class="miscellaneous">
   <metadata>
    <title>CTRL+ALT+DEL Required for Logon</title>
    <affected family="windows"/>
    <description>This definition is used to introduce the OVAL Language.</description>
   </metadata>
   <criteria>
    <criterion test_ref="oval:org.mitre.oval.tutorial:tst:1 comment="The registry key is set to require CTRL+ALT+DEL for Logon"/>
   </criteria>
  </definition>
 </definitions>
 <tests>
  <registry_test id="oval:org.mitre.oval.tutorial:tst:1" version="1" check=“all" comment="The registry key is set to require CTRL+ALT+DEL
     for Logon" xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows">
   <object object_ref="oval:org.mitre.oval.tutorial:obj:1"/>
   <state state_ref="oval:org.mitre.oval.tutorial:ste:1"/>
  </registry_test>
 </tests>
 <objects>
  <registry_object id="oval:org.mitre.oval.tutorial:obj:1" version="1" xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows">
   <hive>HKEY_LOCAL_MACHINE</hive>
   <key>Software\Microsoft\Windows\CurrentVersion\Policies\System</key>
   <name>disablecad </name>
  </registry_object>
 </objects>
 <states>
  <registry_state id="oval:org.mitre.oval.tutorial:ste:1" version="1" xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows">
   <value datatype=“int“ operation="equals">0</value>
  </registry_state>
 </states>
</oval_definitions>
```

Advanced OVAL Topics

- Extended definitions: allow reuse of "building blocks"
- Variables: enable reuse of compliance checks across organizations with varying needs
- Component schemas: define platform-specific tests, objects and states
- Validation: rules to allow automated syntax checking (XML Schema and Schematron)

Demo: OVAL Definition

OVAL Definition Demo

- Write an OVAL Definition for the new minimum password length rule using the Benchmark Editor

- Create the new definition
  - Add extended definition reference - oval:example:def:1
  - Add passwordpolicy_object
  - Add passwordpolicy_state
  - Add passwordpolicy_test
  - Add the criteria

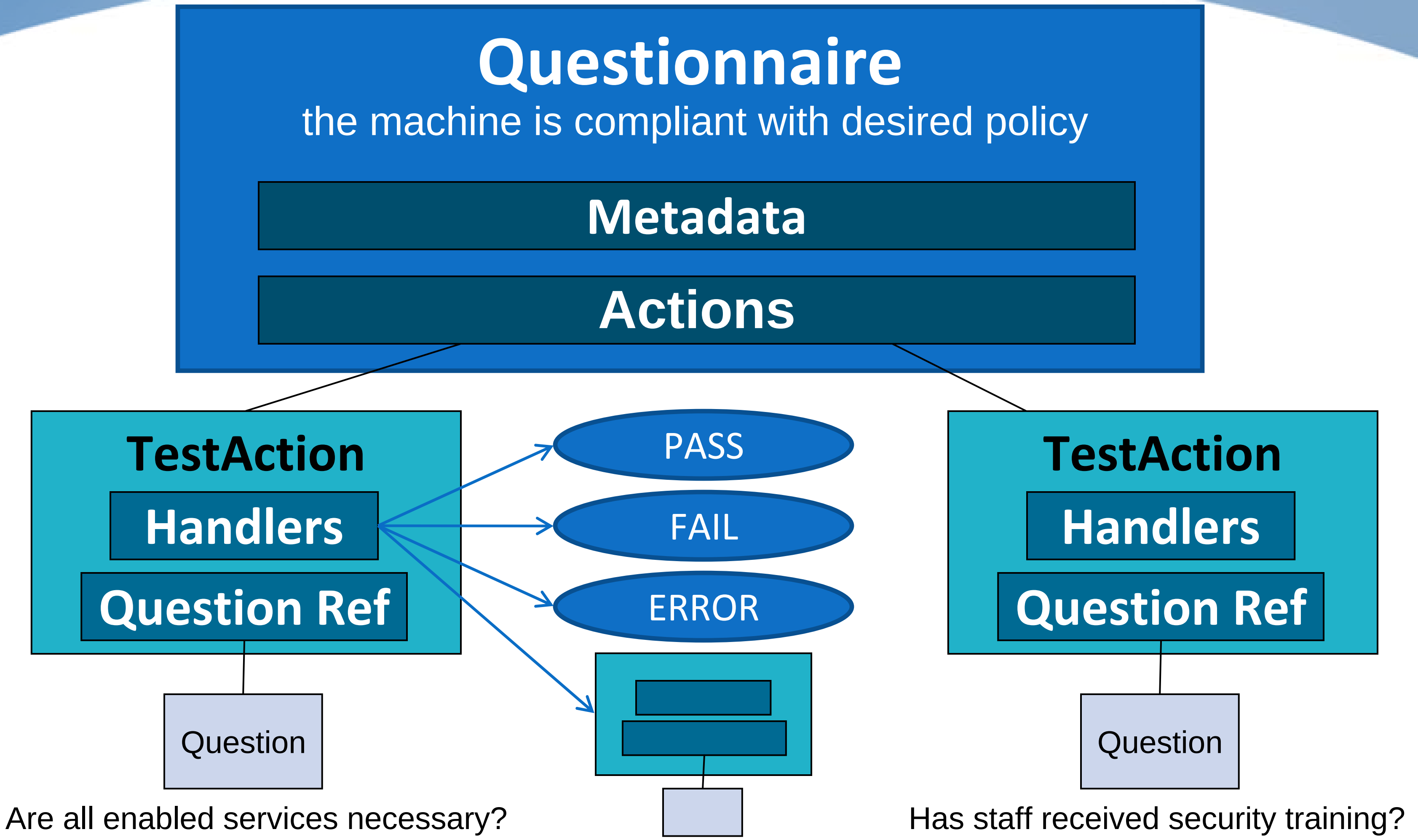
Introduction to OCIL

What is OCIL?

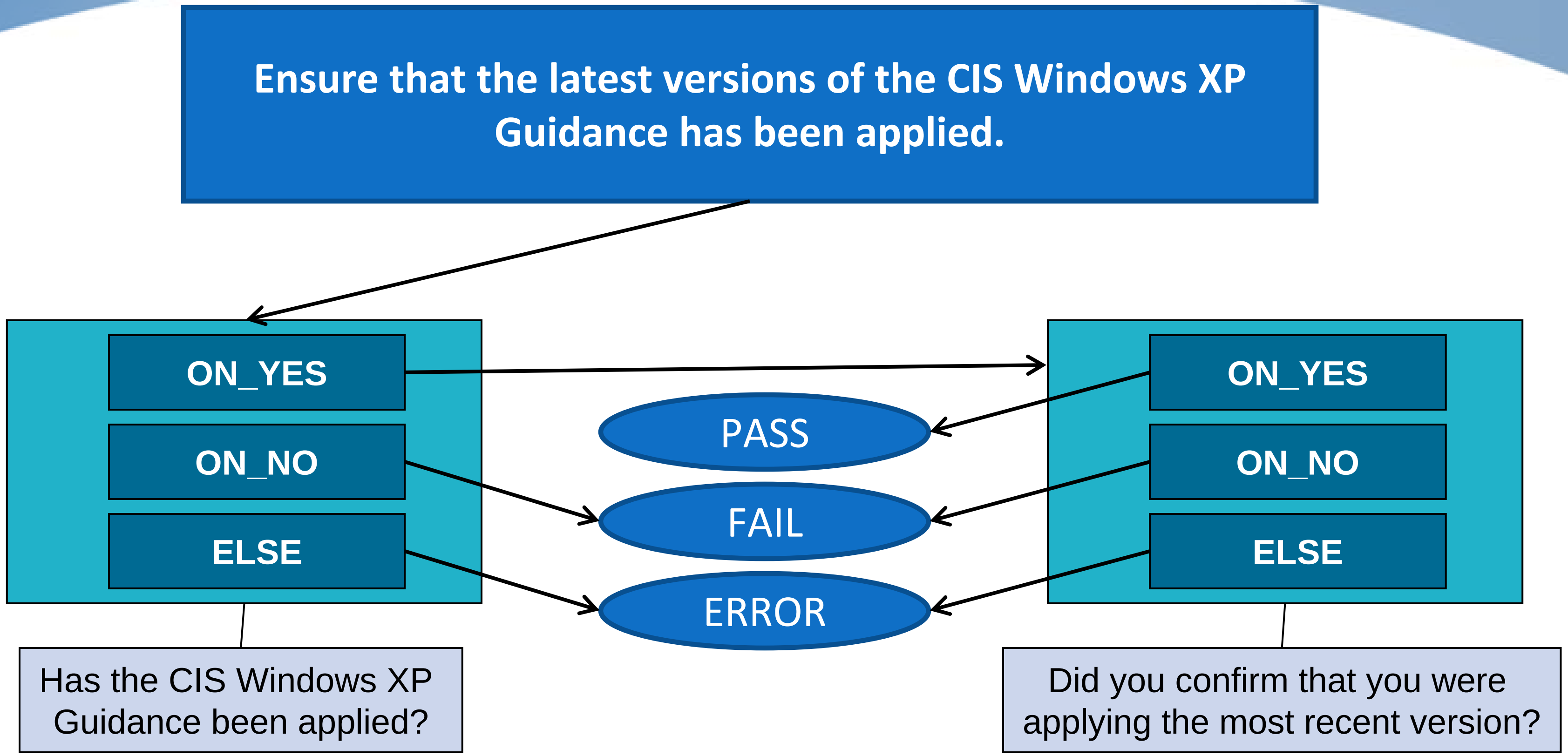
- Open Checklist Interactive Language
- XML-based framework for expressing compliance questionnaires
- Supports questions and follow up questions
- Defines logical constructs to allow lengthy questionnaires to be evaluated and produce a single result
- An emerging specification

http://nvd.nist.gov/ocil.cfm

Structure of an OCIL Definition

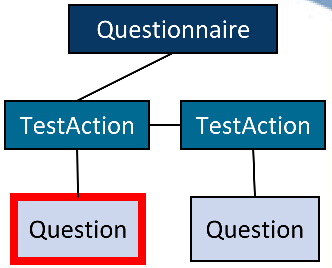


CIS Guidance - OCIL Questionnaire



Ensure that the latest versions of the CIS Windows XP Guidance has been applied.
ON_YES
ON_NO
ELSE
PASS
FAIL
ERROR
ON_YES
ON_NO
ELSE
Has the CIS Windows XP Guidance been applied?
Did you confirm that you were applying the most recent version?

CIS Guidance - Question

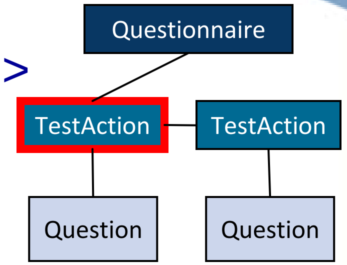


```
<boolean_question
      id="ocil:org.mitre.example:question:1"
      model="MODEL_YES_NO">
  <question_text>Has the CIS Windows XP Guidance
  been applied?
  </question_text>
</boolean_question>
```

MITRE

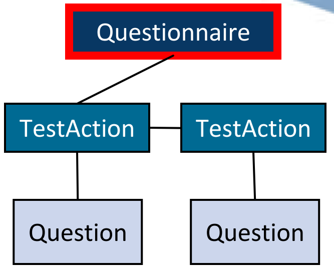
CIS Guidance - TestAction

```
<boolean_question_test_action
  id="ocil:org.mitre.example:testaction:1"
  question_ref="ocil:org.mitre.example:question:1">
  <title>
    Question 1 with follow up question.
  </title>
  <when_true>
    <test_action_ref priority="HIGH">
      ocil:org.mitre.example:testaction:2
    </test_action_ref>
  </when_true>
  <when_false>
    <result>FAIL</result>
  </when_false>
</boolean_question_test_action>
```



MITRE

CIS Guidance - Questionnaire



```
<questionnaire priority="HIGH"
      id="ocil:org.mitre.example:questionnaire:1">
  <title>
    Apply CIS Windows XP Guidance Questionnaire
  </title>
  <actions priority="HIGH" operation="AND">
    <test_action_ref priority="HIGH">
      ocil:org.mitre.example:testaction:1
    </test_action_ref>
  </actions>
</questionnaire>
```

```xml
<ocil xmlns="http://www.mitre.org/ocil/1.0 " >
  <generator>... </generator>
  <questionnaire priority="HIGH" id="ocil:org.mitre.example:questionnaire:1">
    <title>Apply CIS Windows XP Guidance Questionnaire</title>
    <actions priority="HIGH" operation="AND">
      <test_action_ref priority="HIGH">ocil:org.mitre.example:testaction:1</test_action_ref>
    </actions>
  </questionnaire>
  <!-- The test action references a question and defines the action to be taken for each response to the question. -->
  <boolean_question_test_action id="ocil:org.mitre.example:testaction:1" question_ref="ocil:org.mitre.example:question:1">
    <title>Question 1 with follow up question.</title>
    <when_true>
      <test_action_ref priority="HIGH">ocil:org.mitre.example:testaction:2</test_action_ref>
    </when_true>
    <when_false>
      <result>FAIL</result>
    </when_false>
  </boolean_question_test_action>
  <boolean_question_test_action id="ocil:org.mitre.example:testaction:2" question_ref="ocil:org.mitre.example:question:2">
    <notes></notes>
    <when_true>
      <result>PASS</result>
    </when_true>
    <when_false>
      <result>FAIL</result>
    </when_false>
  </boolean_question_test_action>
  <!-- The set of questions to be asked.-->
  <boolean_question id="ocil:org.mitre.example:question:1" model="MODEL_YES_NO">
    <question_text>Has the CIS Windows XP Guidance been applied?</question_text>
  </boolean_question>
  <boolean_question id="ocil:org.mitre.example:question:2" model="MODEL_YES_NO">
    <question_text>Did you confirm that you were applying the most recent version?</question_text>
  </boolean_question>
</ocil>
```

OCIL Interpreter

- Freely available reference implementation
- Demonstrates usability of OCIL
- Easily incorporated into other applications
- Drives the development of the schema
- Validate & test content
- Reduce the cost of adoption

http://sourceforge.net/projects/interactive

MITRE

Conclusion

- Compliance checks bring automated compliance assessment to benchmarking
- Remove guesswork
- OVAL standard understood by wide range of tools
- Emerging specifications are expanding capabilities