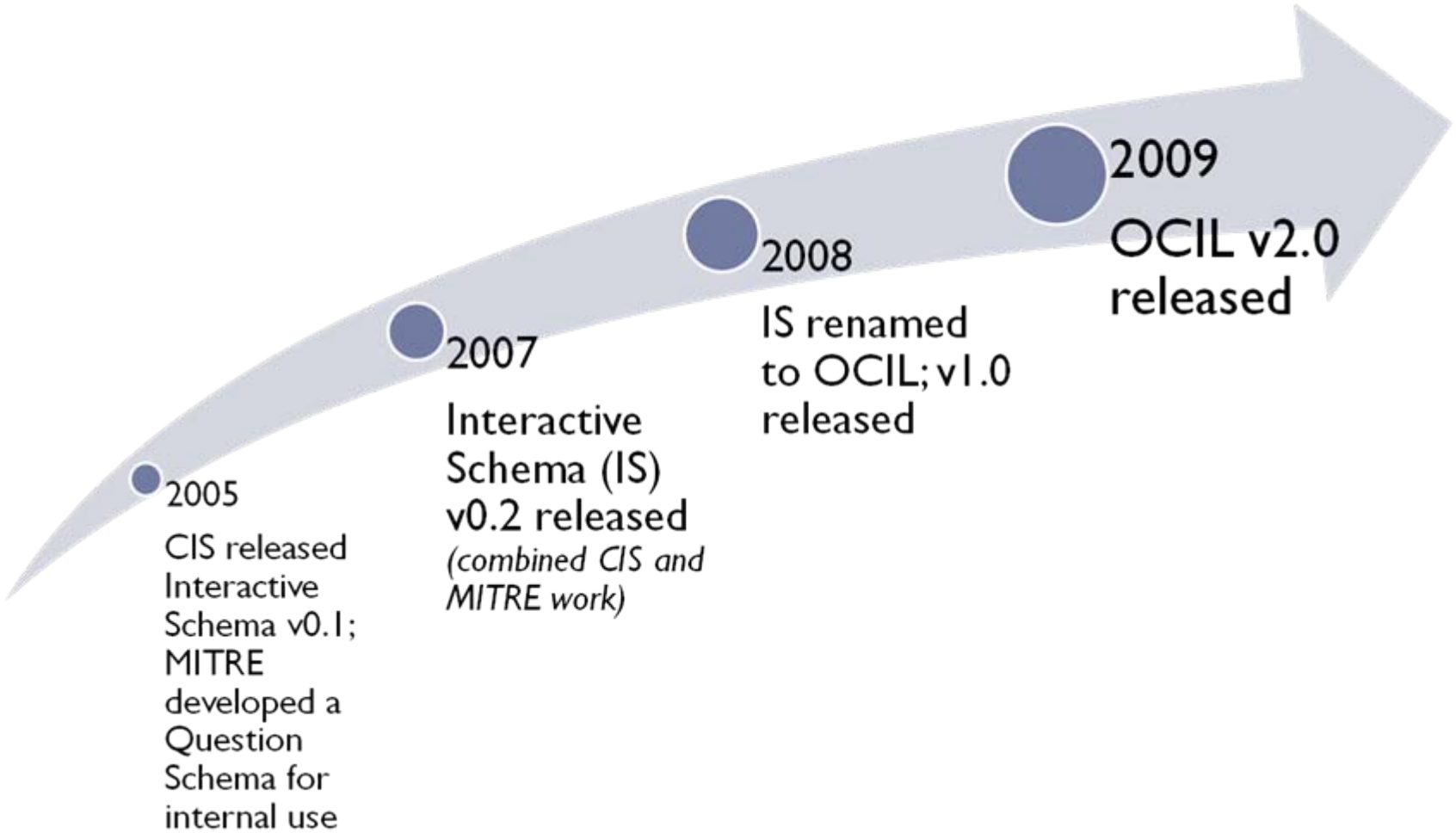
Open Checklist Interactive Language

An Introduction to **OCIL**

Maria Casipe
10/26/2009

History of OCIL



Security Automation Standards

- XCCDF

  [eXtensible Configuration Checklist Description Format]

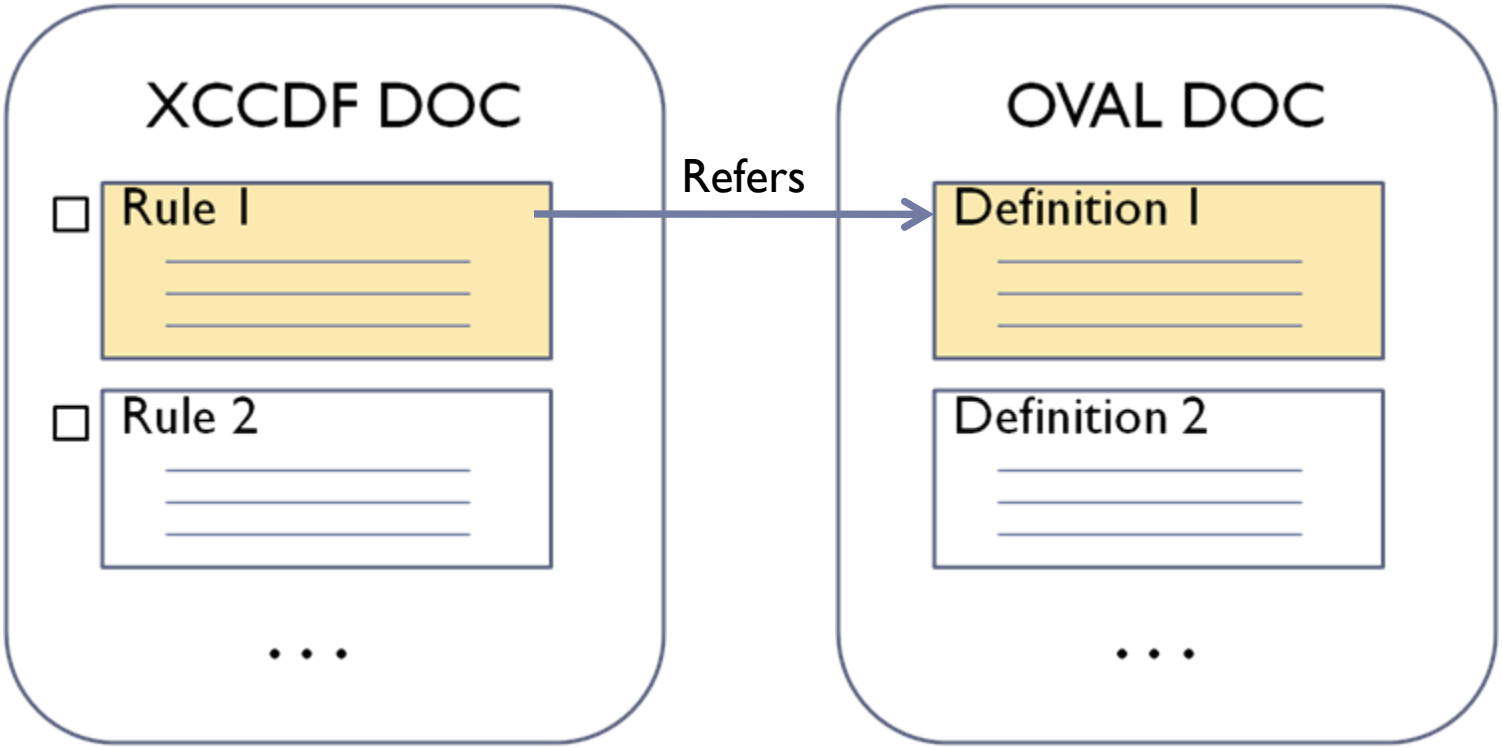
  A specification language for writing security checklists, benchmarks, and related kinds of documents.

- OVAL

  [Open Vulnerability and Assessment Language]

  A specification language for writing machine-readable rules to check a state of the system.

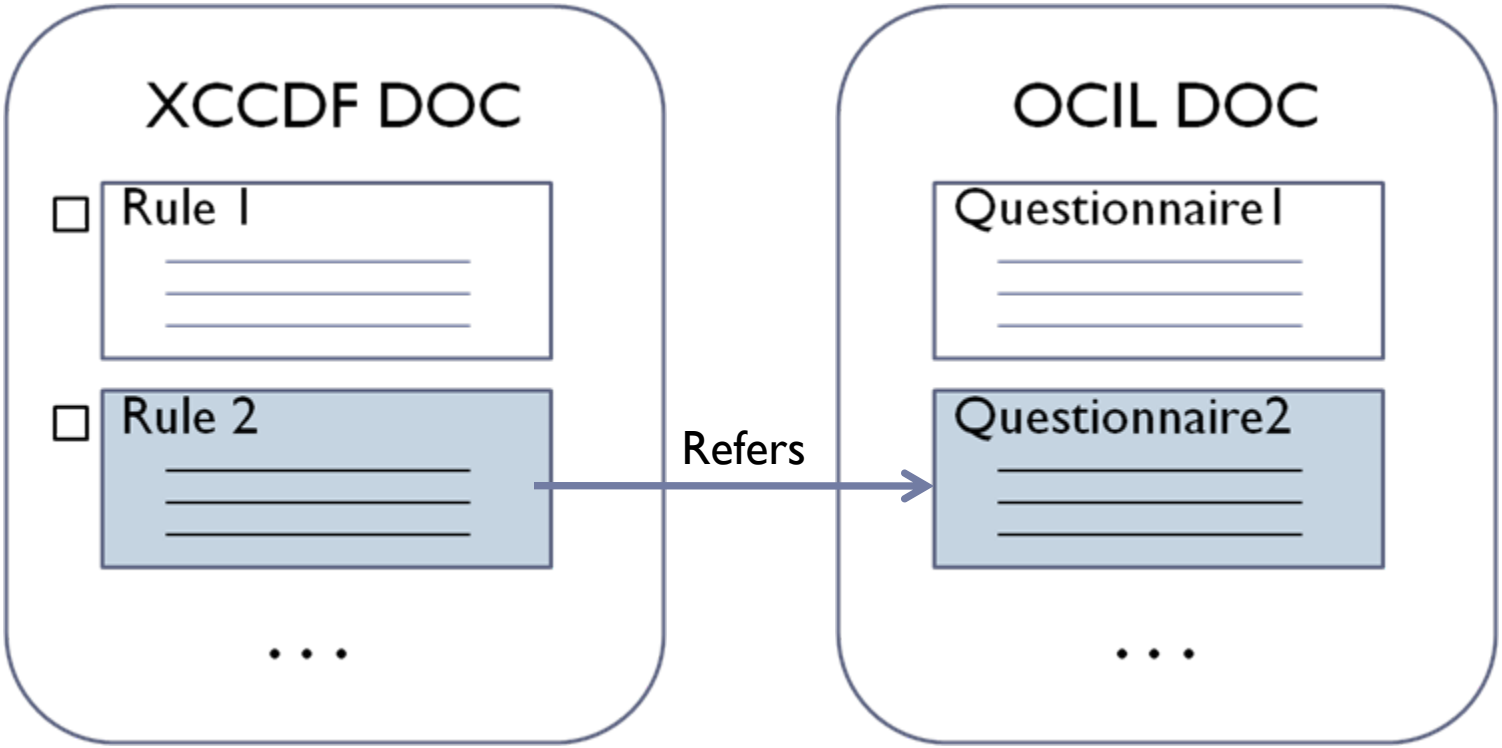
XCCDF and OVAL Documents



Rule 1: Minimum password length must be 12.

Definition 1: Check registry that minimum password length is set to 12.

XCCDF and OCIL Documents



Rule 2: **All laptops must be locked with a cable lock.**

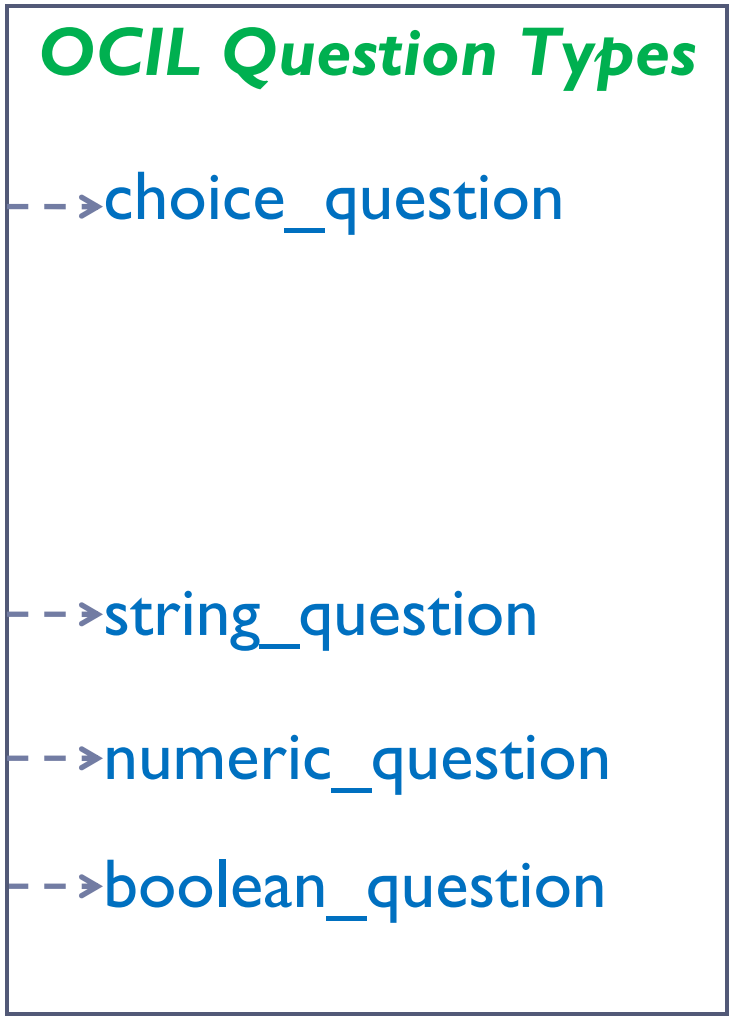
Questionnaire 2: Check with security officer that all laptops have been locked with a cable lock.

Basic Features of OCIL

Sample Questionnaire

Rule 2: All laptops must be locked with a cable lock.

1. What type of computer is it?
   a) Laptop
   b) Desktop
   c) Workstation
   d) Server
   e) Not Listed
2. Who is responsible for the computer? *Answer must be in the following format: last name, first name (e.g. Doe, Jane).*
3. What is the computer's barcode number?
4. Is the laptop locked with a cable lock?

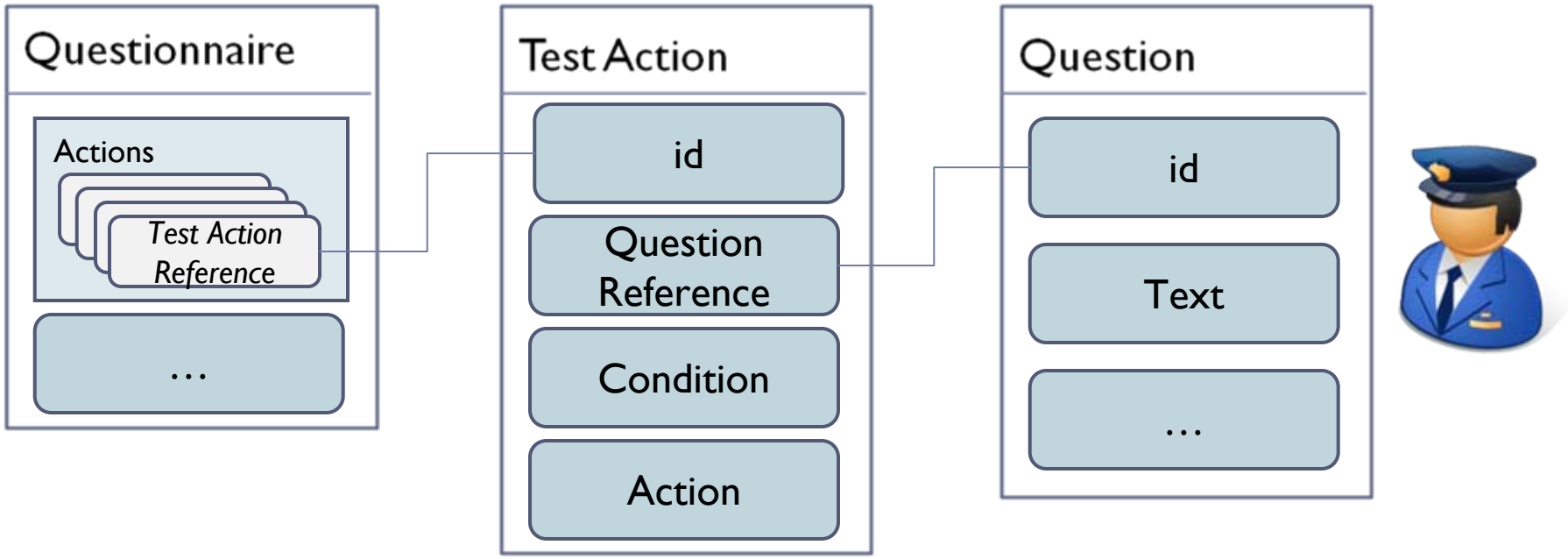


Example 1:
A Questionnaire with A Single Question

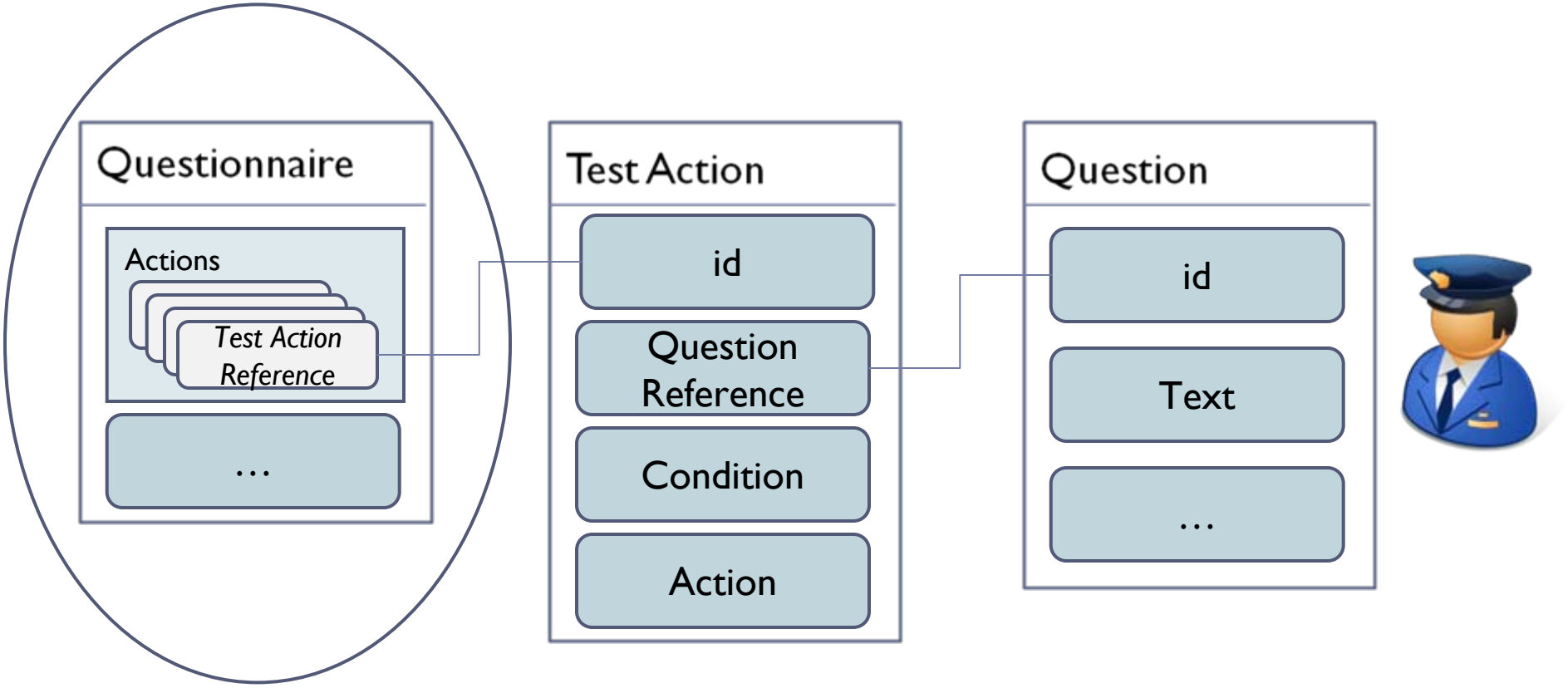
All laptops must be locked with a cable lock.

1. Is the laptop locked with a cable lock?

Core OCIL Objects



Creating an OCIL Questionnaire: Step 1



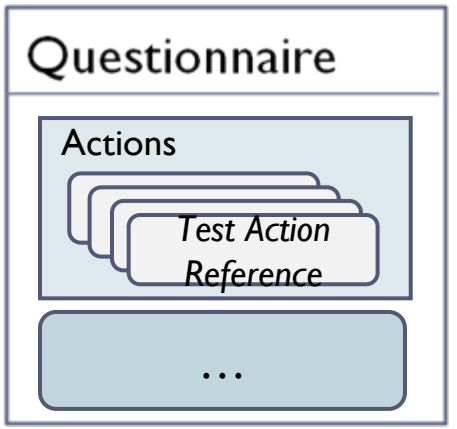
STEP 1: Create a Questionnaire.

Step 1: Create a Questionnaire

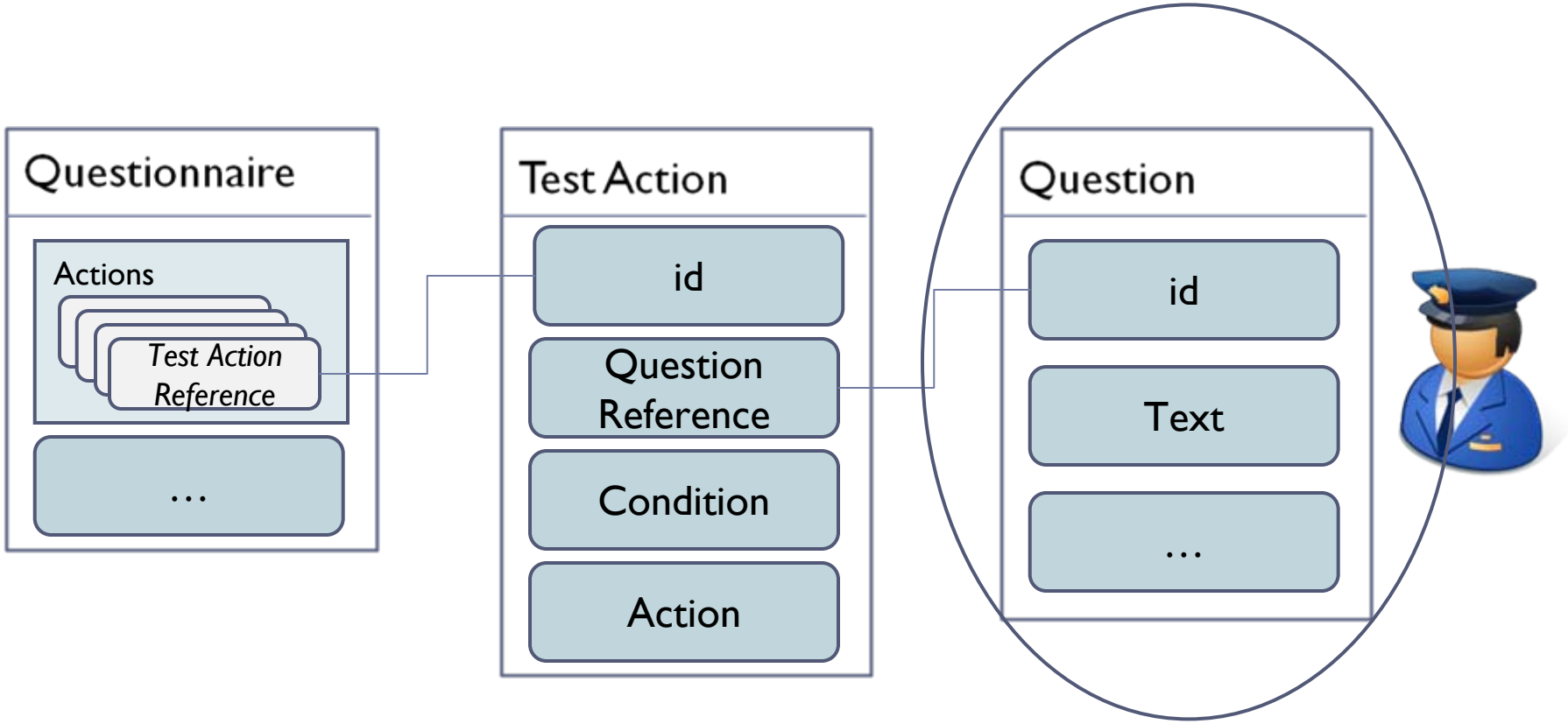
```
<questionnaire id="ocil:mitre.org:questionnaire:1">
    <title>
      All laptops must be locked with a cable lock
    </title>
    <description>
      The following questionnaire interviews a security officer to check
      that all laptops have been locked with a cable lock.
    </description>
    <references>
      <reference href="http://cce.mitre.org">CCE-0123-4 </reference>
    </references>

        . . .

  </questionnaire>
```



Creating an OCIL Questionnaire: Step 2

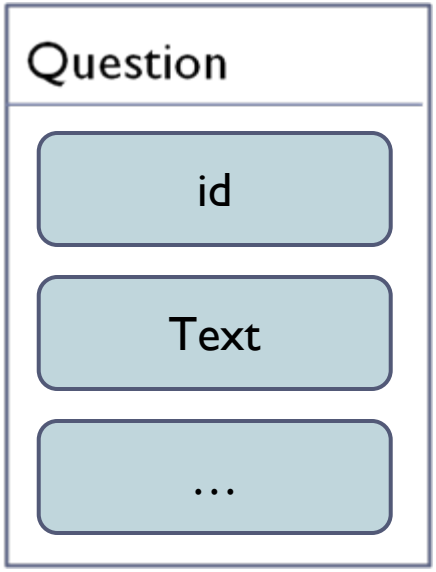


STEP 2: Create a Question.

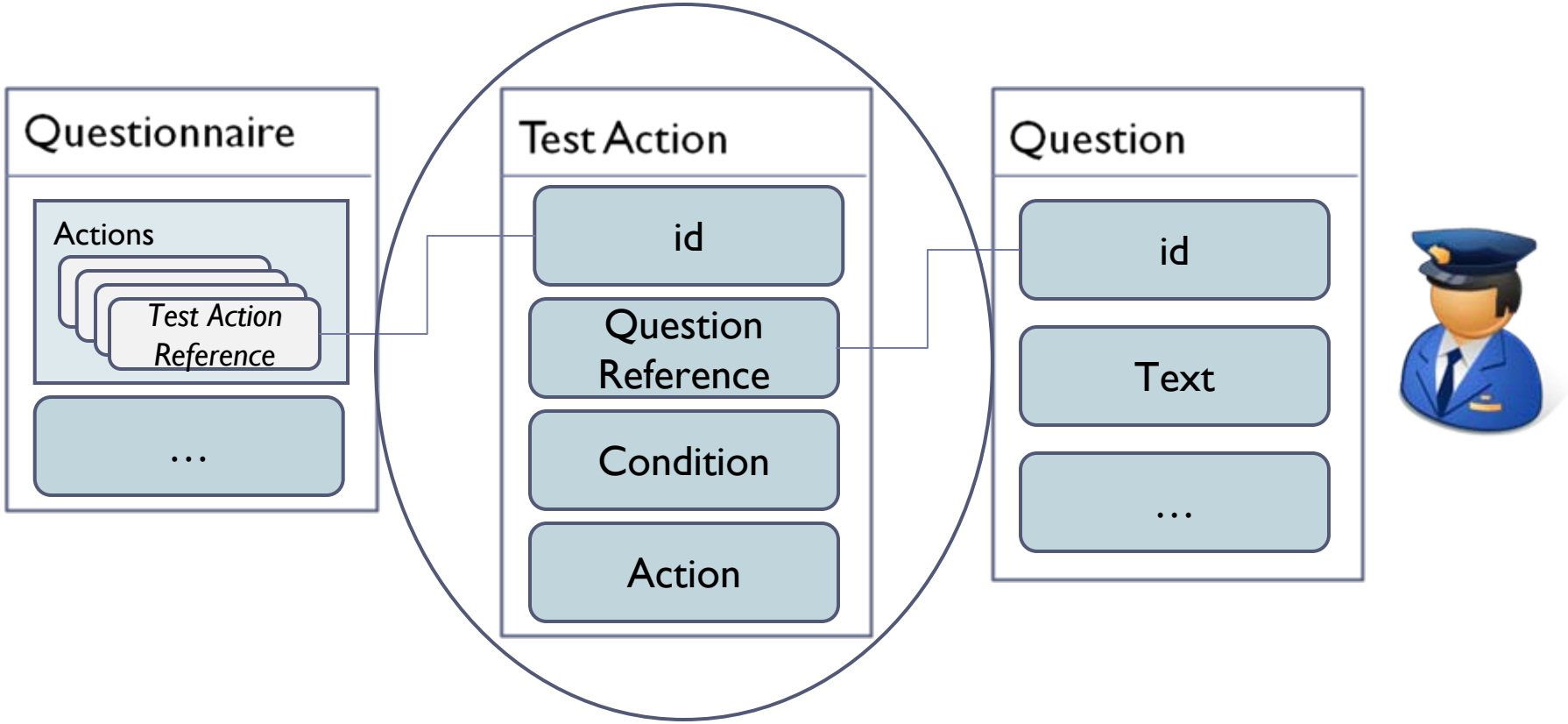
Step 2: Create a Question

Is the laptop locked with a cable lock?

```
<boolean_question id="ocil:mitre.org:question:4"
    model="MODEL_YES_NO">
    <question_text>
     Is the laptop locked with a cable lock?
    </question_text>
</boolean_question>
```



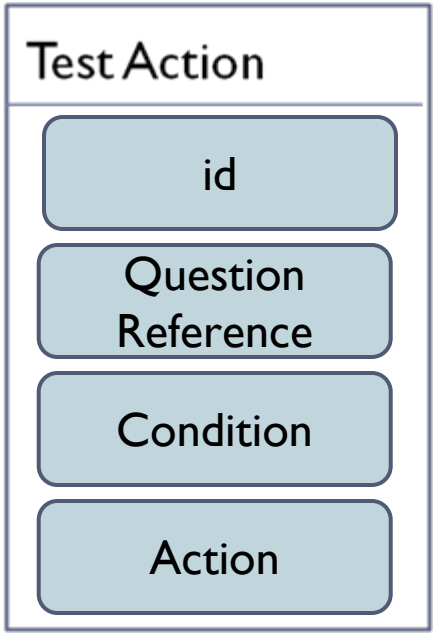
Creating an OCIL Questionnaire: Step 3



STEP 3: Create a Test Action

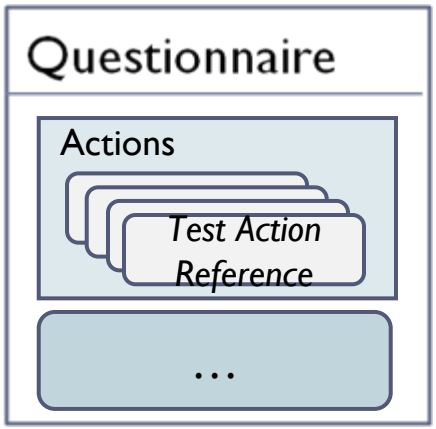
Step 3: Create a Test Action

```
<boolean_question_test_action id="ocil:mitre.org:testaction:4"
    question_ref="ocil:mitre.org:question:4" >
    <when_true>
            <result>PASS</result>
    </when_true>
    <when_false>
            <result>FAIL</result>
    </when_false>
    <when_not_applicable>
            <result>NOT_APPLICABLE</result>
    </when_not_applicable>
    <when_not_tested>
            <result>NOT_TESTED</result>
    </when_not_tested>
</boolean_question_test_action>
```



Step 4: Link Questionnaire and Test Action

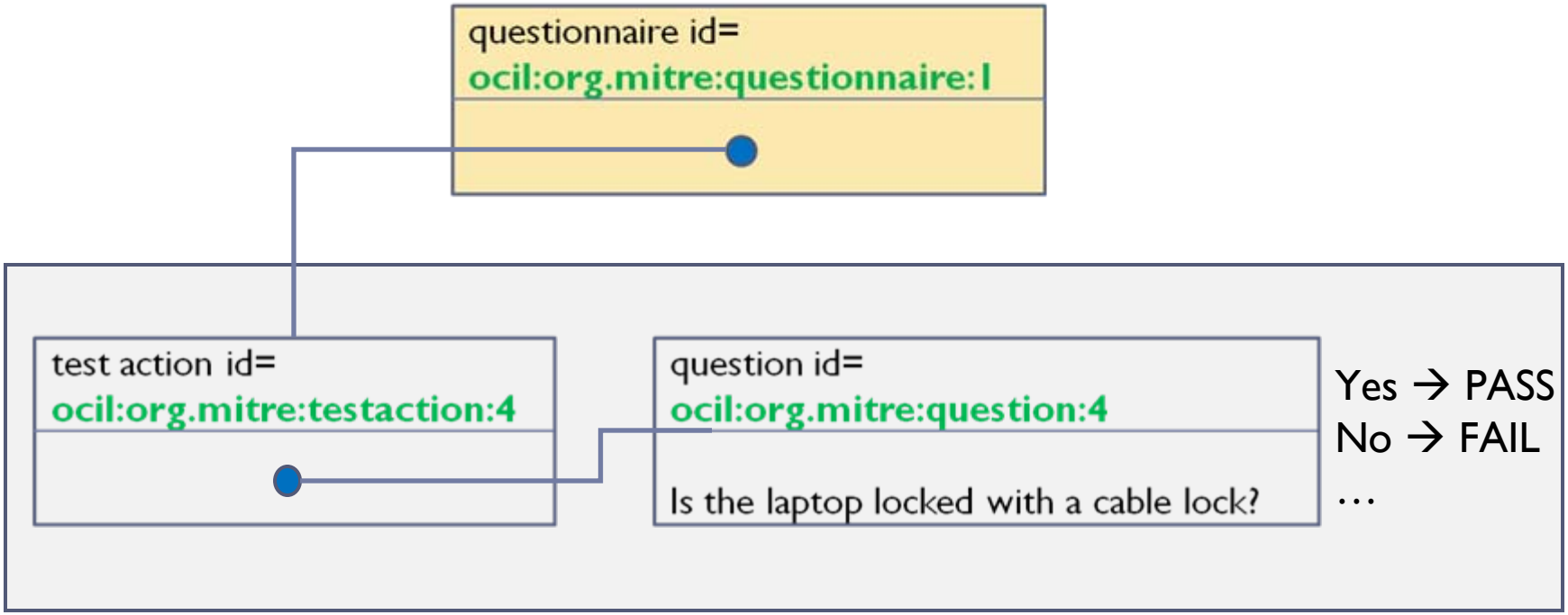
```
<questionnaire id="ocil:mitre.org:questionnaire:1">
    <title>
      All laptops must be locked with a cable lock
    </title>
    <description>
      The following questionnaire interviews a security officer to check
      that all laptops have been locked with a cable lock.
    </description>
    <references>
      <reference href="http://cce.mitre.org">CCE-0123-4 </reference>
    </references>
    <actions>
      <test_action_ref>
        ocil:mitre.org:testaction:4
      </test_action_ref>
    </actions>
  </questionnaire>
```



Putting it all together:
A Questionnaire with A Single Question

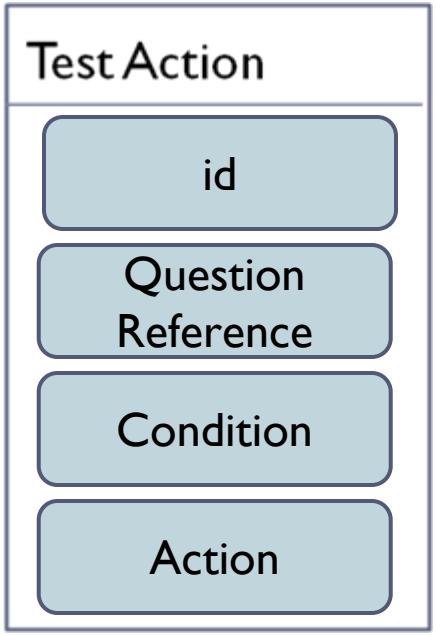
All laptops must be locked with a cable lock.

1) Is the laptop locked with a cable lock?



Back to the Test Action…

```
<boolean_question_test_action id="ocil:mitre.org:testaction:4"
    question_ref="ocil:mitre.org:question:4" >
    <when_true>
            <result>PASS</result>
    </when_true>
    <when_false>
            <result>FAIL</result>
    </when_false>
    <when_not_applicable>
            <result>NOT_APPLICABLE</result>
    </when_not_applicable>
    <when_not_tested>
            <result>NOT_TESTED</result>
    </when_not_tested>
</boolean_question_test_action>
```



Example 2:
A Questionnaire with Multiple Questions

All laptops must be locked with a cable lock.

1. What type of computer is it?
   a) Laptop
   b) Desktop
   c) Workstation
   d) Server
   e) Not Listed
2. Is the laptop locked with a cable lock?

Add a Choice Question

1. What type of computer is it?
   a) Laptop
   b) Desktop
   c) Workstation
   d) Server
   e) Not Listed

```
<choice_question id="ocil:mitre.org:question:3"
  default_answer_ref="ocil:mitre.org:choice:1">
    <question_text>What type of computer is it?</question_text>
    <choice id="ocil:mitre.org:choice:1">Laptop</choice>
    <choice id="ocil:mitre.org:choice:2">Desktop</choice>
    <choice id="ocil:mitre.org:choice:3">Workstation</choice>
    <choice id="ocil:mitre.org:choice:4">Server</choice>
    <choice id="ocil:mitre.org:choice:5">Not Listed</choice>
</choice_question>
```

Add a Choice Question Test Action

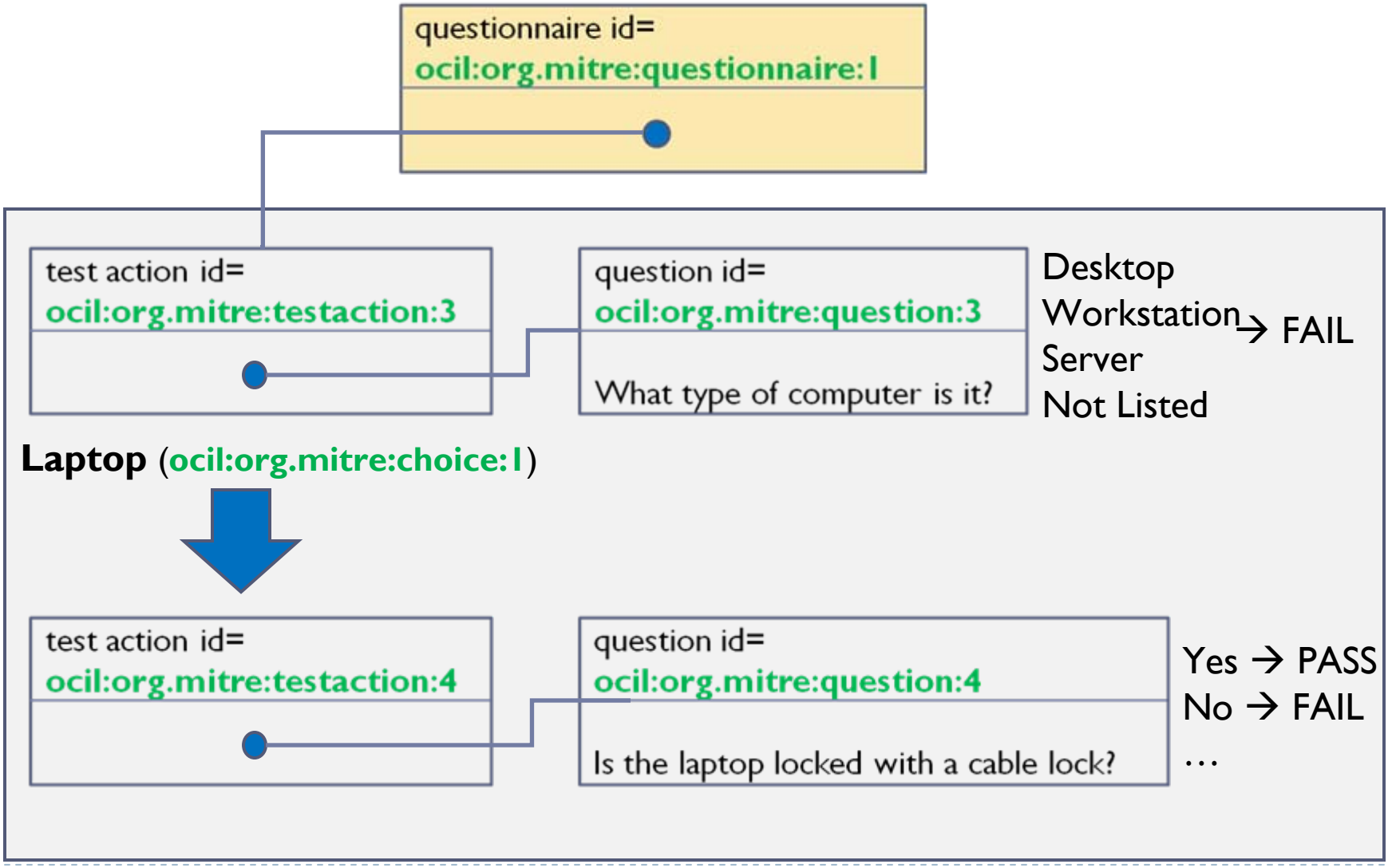
```
<choice_question_test_action id="ocil:mitre.org:testaction:3"
   question_ref="ocil:mitre.org:question:3”>
  <when_choice>
    <test_action_ref>ocil:mitre.org:testaction:4</test_action_ref>
    <choice_ref>ocil:mitre.org:choice:1</choice_ref>
  </when_choice>
  <when_choice>
    <result>FAIL</result>
    <choice_ref>ocil:mitre.org:choice:2</choice_ref>
    <choice_ref>ocil:mitre.org:choice:3</choice_ref>
    <choice_ref>ocil:mitre.org:choice:4</choice_ref>
    <choice_ref>ocil:mitre.org:choice:5</choice_ref>
  </when_choice>
</choice_question_test_action>
```

Choice 1: Laptop
Choice 2: Desktop
Choice 3: Workstation
Choice 4: Server
Choice 5: Not Listed

Modifying Questionnaire 1

```
<questionnaire id="ocil:mitre.org:questionnaire:1“>
    <title>All laptops must be locked with a cable lock.</title>
    <description>
      The following questionnaire interviews a security officer to check
      that all laptops has been locked with a cable lock.
    </description>
    <references>
      <reference href=“http://cce.mitre.org">CCE-0123-4 </reference>
    </references>
    <actions>
      <test_action_ref>
        ocil:mitre.org:testaction:3
      </test_action_ref>
    </actions>
  </questionnaire>
```

Putting it all together:
A Questionnaire with Multiple Questions

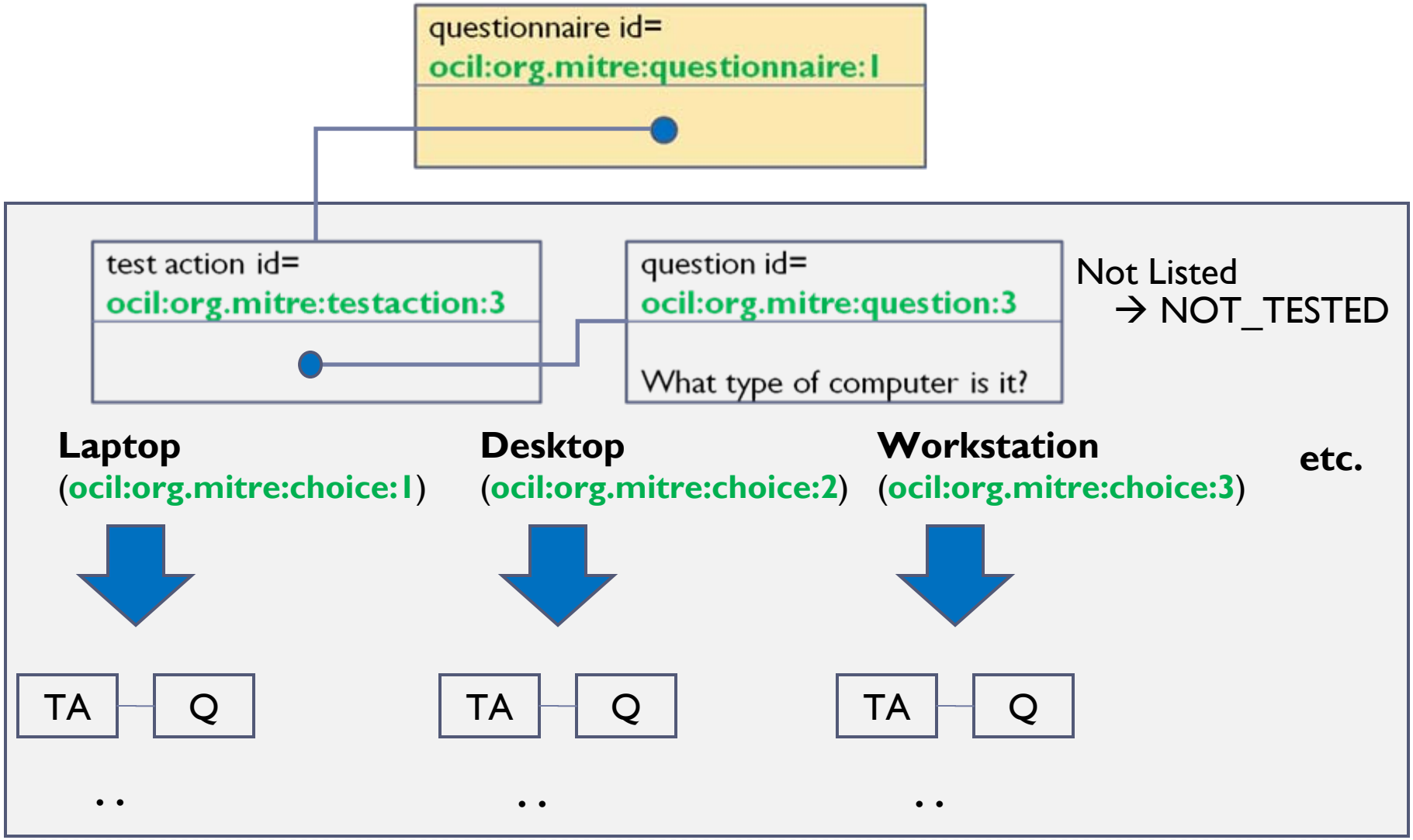


Back to the Choice Question Test Action…

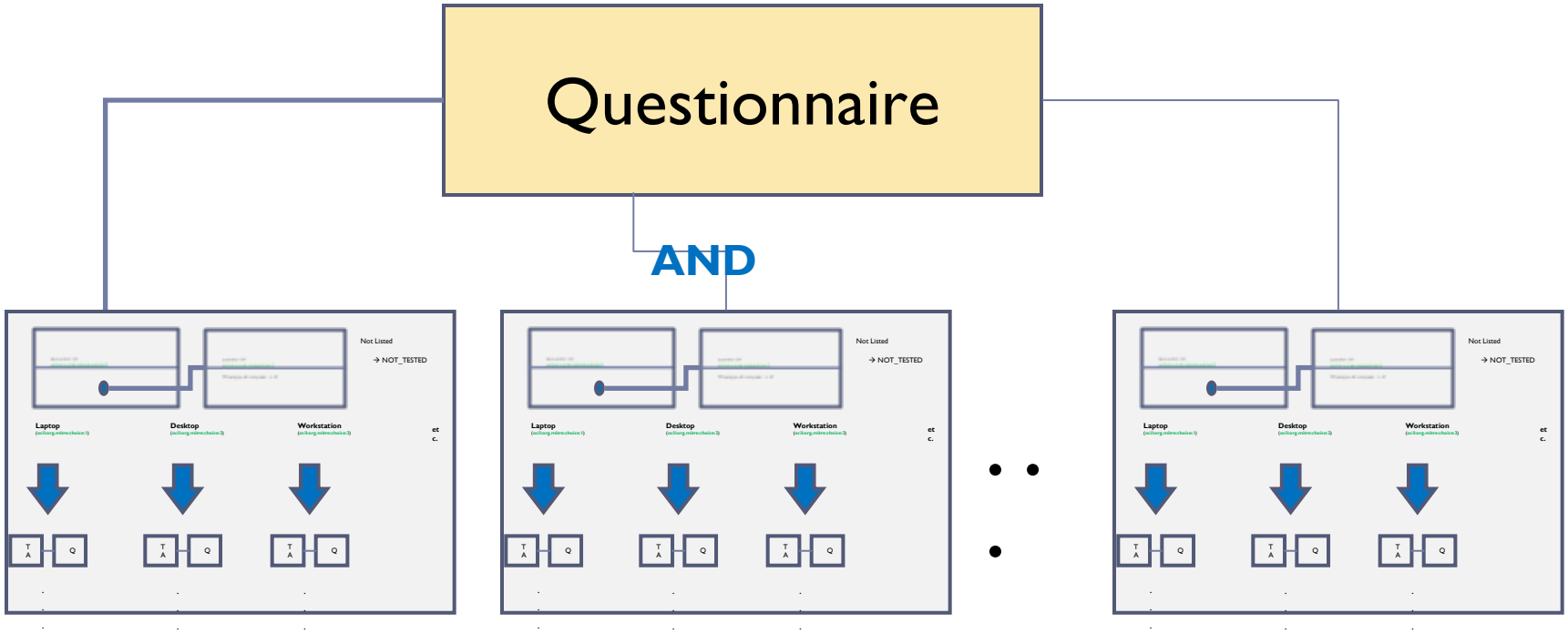
```
<choice_question_test_action id="ocil:mitre.org:testaction:3"
   question_ref="ocil:mitre.org:question:3”>
  <when_choice>
    <test_action_ref>ocil:mitre.org:testaction:4</test_action_ref>
    <choice_ref>ocil:mitre.org:choice:1</choice_ref>
  </when_choice>
  <when_choice>
    <result>FAIL</result>
    <choice_ref>ocil:mitre.org:choice:2</choice_ref>
    <choice_ref>ocil:mitre.org:choice:3</choice_ref>
    <choice_ref>ocil:mitre.org:choice:4</choice_ref>
    <choice_ref>ocil:mitre.org:choice:5</choice_ref>
  </when_choice>
</choice_question_test_action>
```

Choice 1: Laptop
Choice 2: Desktop
Choice 3: Workstation
Choice 4: Server
Choice 5: Not Listed

Example 3:
A Questionnaire – 1 Branch, ***Multiple Paths***

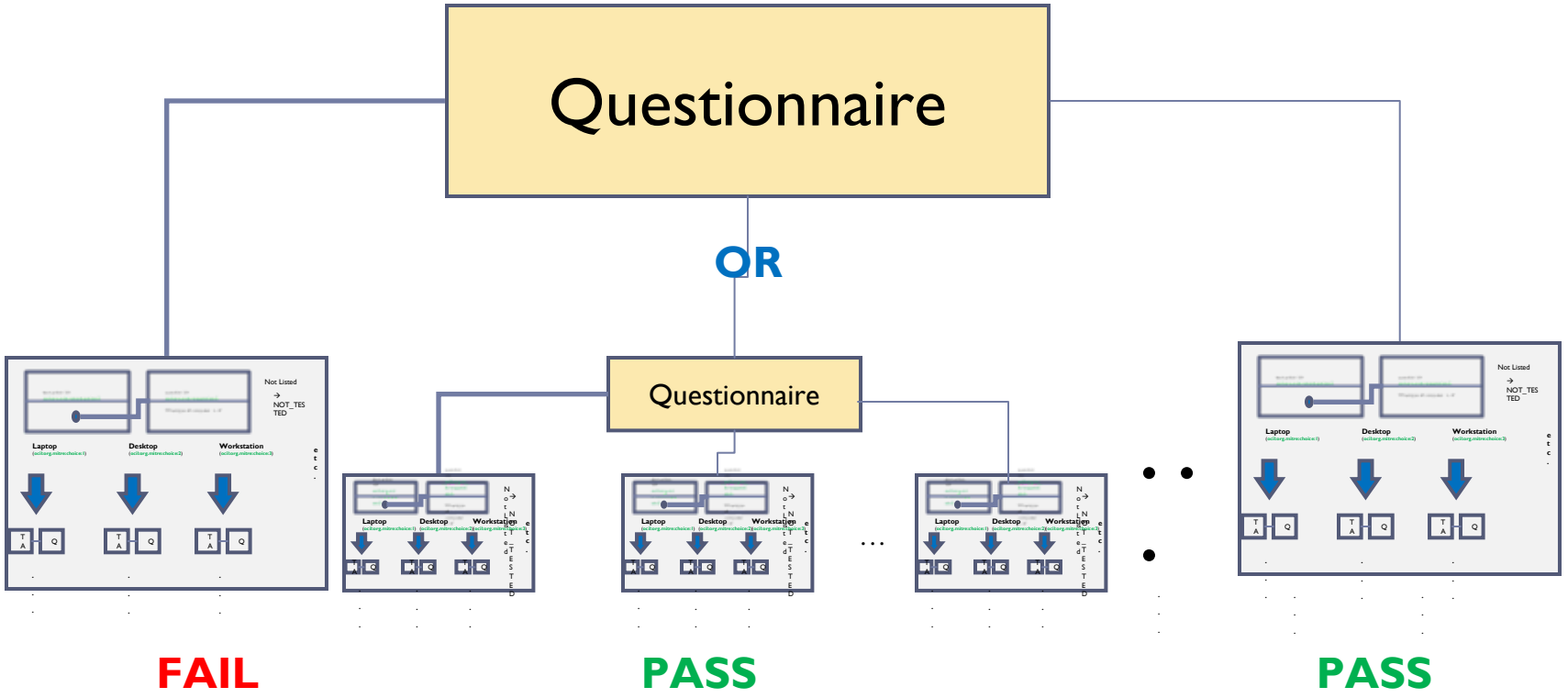


Example 4:
*A Questionnaire with **Multiple Branches***



LOGICAL OPERATIONS:
AND / OR / NOT

Example 5:
A Questionnaire with ***Child Questionnaires***



LOGICAL OPERATIONS:
AND / OR / NOT

Example Questionnaire with Multiple Branches and Child Questionnaires

```
<questionnaire id="ocil:mitre.org:questionnaire:1“>
    <title>All laptops must be locked with a cable lock.</title>
    <description>
      The following questionnaire interviews a security officer to check
      that all laptops has been locked with a cable lock.
    </description>
    <references>
      <reference href=“http://cce.mitre.org">CCE-0123-4 </reference>
    </references>
    <actions negate="false" operation="AND">
      <test_action_ref  negate="false">
        ocil:mitre.org:testaction:3
      </test_action_ref>
     <test_action_ref negate="false">
        ocil:mitre.org:questionnaire:2
      </test_action_ref>
      <test_action_ref negate="false">
        ocil:mitre.org:testaction:4
      </test_action_ref>
      <test_action_ref negate="false">
        ocil:mitre.org:questionnaire:3
      </test_action_ref>
    </actions>
  </questionnaire>
```

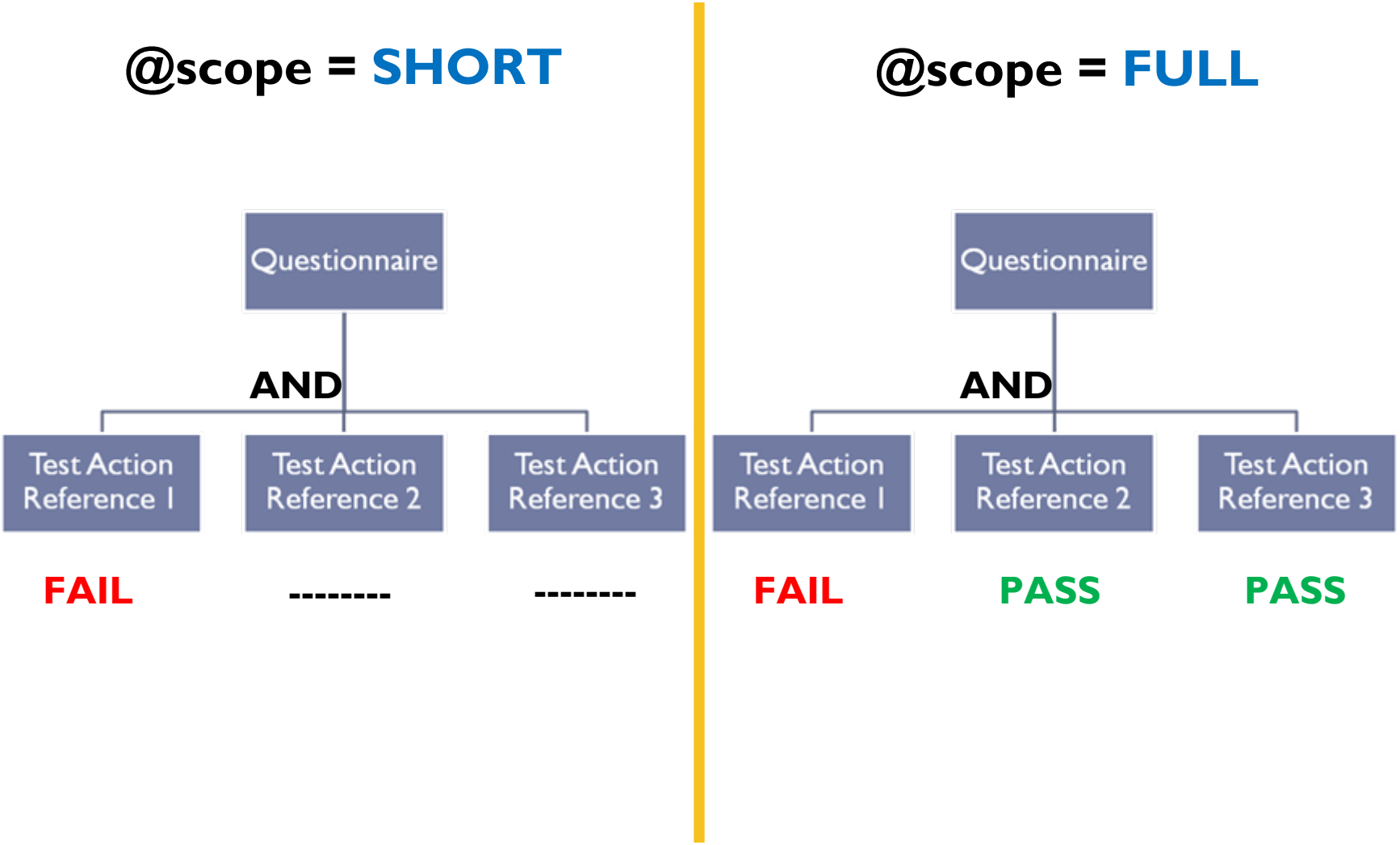
Advance Features of OCIL

Including Metadata

```
<generator>
  <schema_version>2.0</schema_version>
  <timestamp>2009-10-26T11:34:01</timestamp>
  <author>
    <name>Jane Doe</name>
  </author>
</generator>

<document>
  <title>Sample OCIL Document</title>
  <description>
        The following is a sample OCIL document used in the
        Introduction to OCIL Tutorial.
  </description>
</document>
```

Controlling Evaluation



Including Artifacts

```
<boolean_question_test_action id="ocil:mitre.org:testaction:4"
    question_ref="ocil:mitre.org:question:4" >
  <when_true>
    <result>PASS</result>
  </when_true>
  <when_false>
    <result>FAIL</result>
    <artifacts>
      <artifact id="ocil:mitre.org:artifact:16" datatype="TEXT" required="true">
        <title>Other Physical Protection</title>
        <description>Describes any other protection that the system may have, e.g.
          inside a locked box.</description>
      </artifact>
    </artifacts>
  </when_false>
  …
</boolean_question_test_action>
```

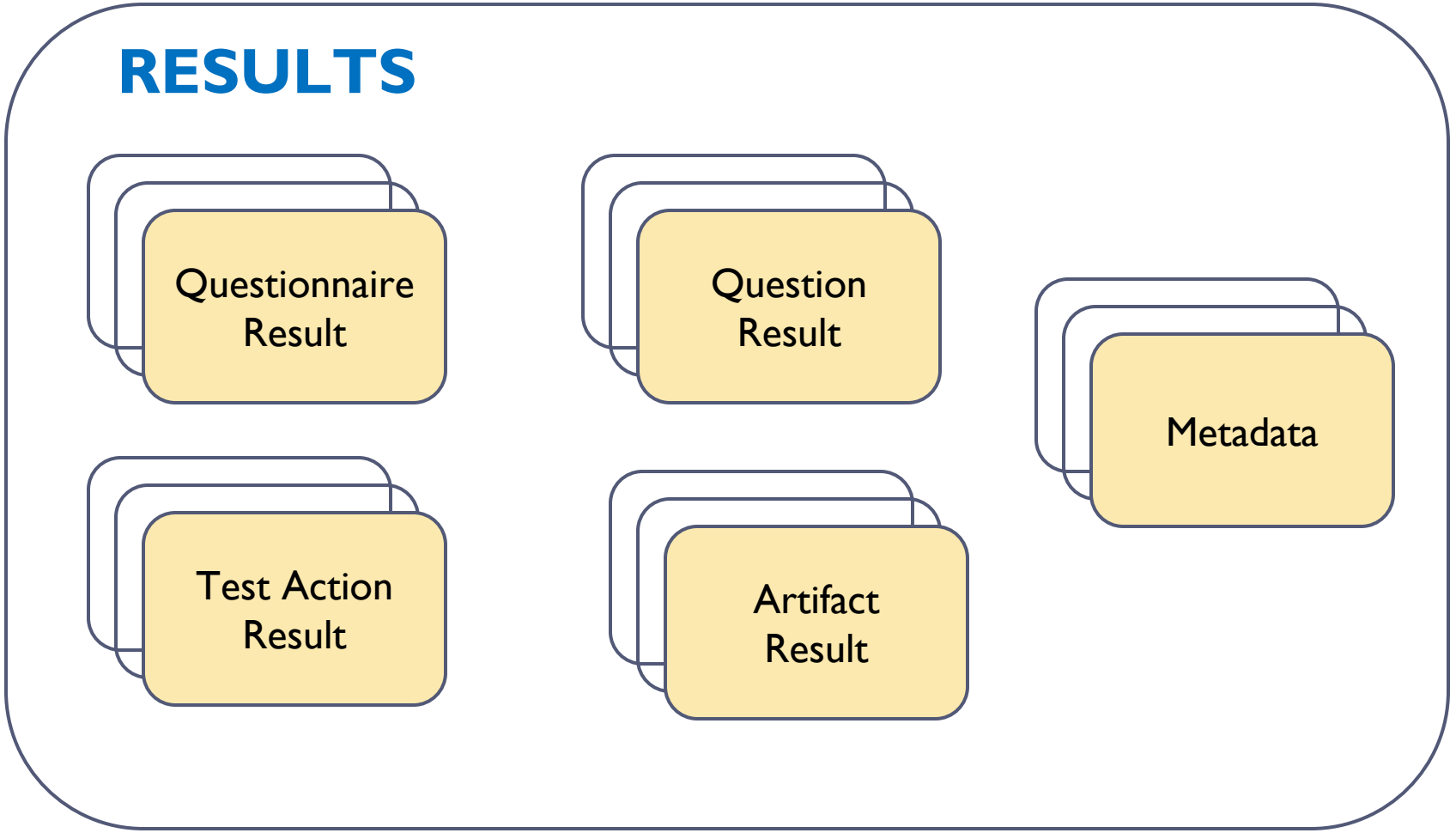
Adding Instructions

```
<boolean_question id="ocil:mitre.org:question:4"
    model="MODEL_YES_NO">
    <question_text>
     Is the laptop locked with a cable lock?
    </question_text>
    <instructions>
        <title>The following contains instructions on how to check
         that the cable lock has been locked.</title>
        <step>Check that a cable lock has been installed on the
         system.</step>
        <step>Check that you cannot remove the system from its
         location.</step>
    </instructions>
</boolean_question>
```

Setting Variables

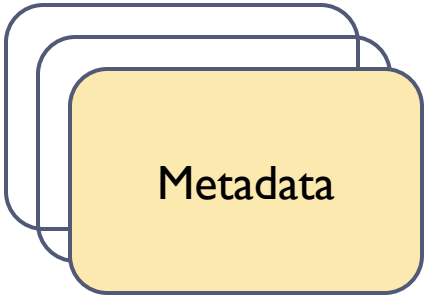
- Constant Variables
- Local Variables
- External Variables

Recording Evaluation



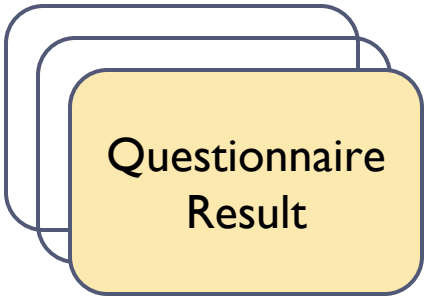
Results Metadata

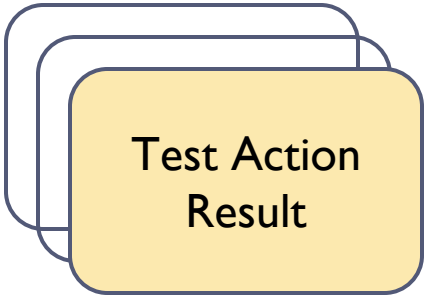
1. Title
2. Targets
3. Start time
4. End time



Questionnaire and Test Action Results

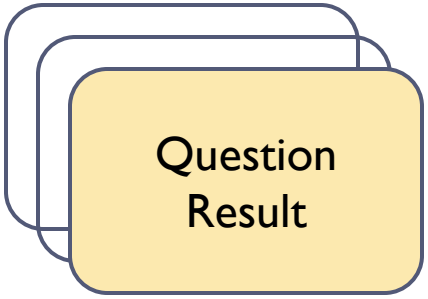
1. Questionnaire / Test Action Reference
2. Result Values:
   a) PASS
   b) FAIL
   c) UNKNOWN
   d) NOT_TESTED
   e) NOT_APPLICABLE
   f) ERROR





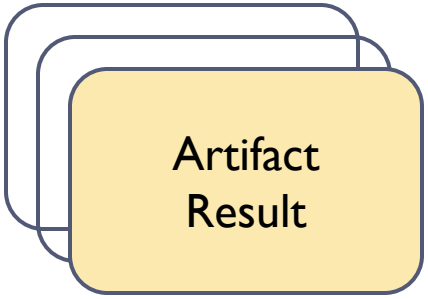
Question Results

1. Question reference
2. User Response



Artifact Results

1. Artifact Reference
2. Timestamp
3. Submitter / Provider



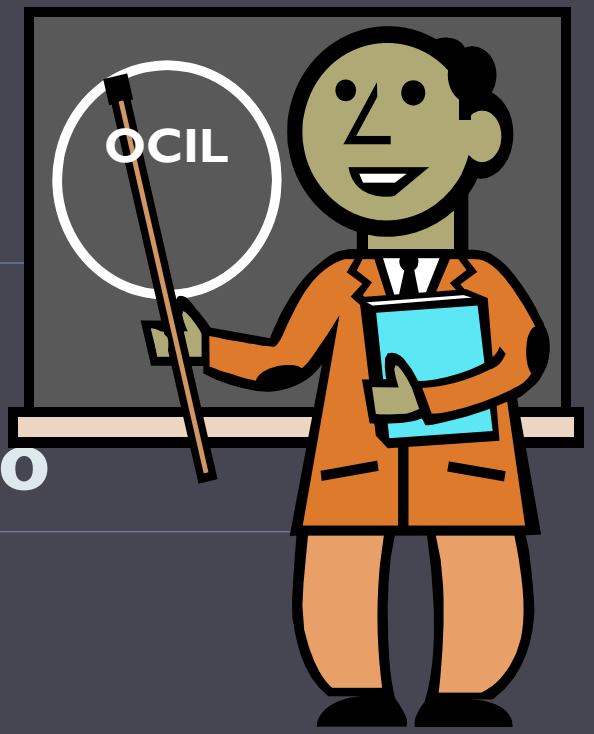
Sample Results

```
<results>
  <questionnaire_results>
    <questionnaire_result questionnaire_ref="ocil:mitre.org:questionnaire:1" result="PASS"/>
    <questionnaire_result questionnaire_ref="ocil:mitre.org:questionnaire:2" result="PASS"/>
  </questionnaire_results>
  <test_action_results>
    <test_action_result test_action_ref="ocil:mitre.org:testaction:22" result="PASS"/>
    <test_action_result test_action_ref="ocil:mitre.org:testaction:222" result="PASS"/>
    <test_action_result test_action_ref="ocil:mitre.org:testaction:26" result="PASS"/>
  </test_action_results>
  <question_results>
    <boolean_question_result response="ANSWERED" question_ref="ocil:mitre.org:question:22">
      <answer>true</answer>
    </boolean_question_result>
    <boolean_question_result response="ANSWERED" question_ref="ocil:mitre.org:question:222">
      <answer>true</answer>
    </boolean_question_result>
    <boolean_question_result response="ANSWERED" question_ref="ocil:mitre.org:question:26">
      <answer>true</answer>
    </boolean_question_result>
  </question_results>
</results>
```

Features

- BASICS:
  - Building Simple Questionnaires (e.g. A Single Path)
  - Building Complex Questionnaires
    - Multiple Paths
    - Multiple Branches
    - Logical Operations
    - Child Questionnaires
- ADVANCE:
  - Including Metadata
  - Controlling Evaluation
  - Including Artifacts
  - Adding Instructions
  - Setting Variables
  - Recording Evaluation
  - …

OCIL Reference Implementation Demo



What's Ahead?

- Further Development
  - Support for Targets
  - Enhancements on the Artifact and Variable Objects
  - OCIL Content and Documentation
- Inclusion to SCAP 2010

Resources

OCIL Specification and Files
http://scap.nist.gov/specifications/ocil/

OCIL Interpreter
http://sourceforge.net/projects/interactive/

OCIL Feedback
ocil-feedback-list@lists.mitre.org

OCIL Developer
ocil-developer-list@lists.mitre.org

OCIL Developer List Archive
http://n2.nabble.com/OCIL-Open-Checklist-Interactive-Language-f3231744.html

Summary

- PART 1:
  - Basic Features of OCIL
    - Building Simple Questionnaires
    - Building Complex Questionnaires
  - Advance Features of OCIL
    - Including Metadata
    - Controlling Evaluation
    - Including Artifacts
    - Adding Instructions
    - Setting Variables
    - Recording Evaluation
- PART 2:
  - OCIL Reference Implementation Demo
  - Future of OCIL
  - Resources

Questions