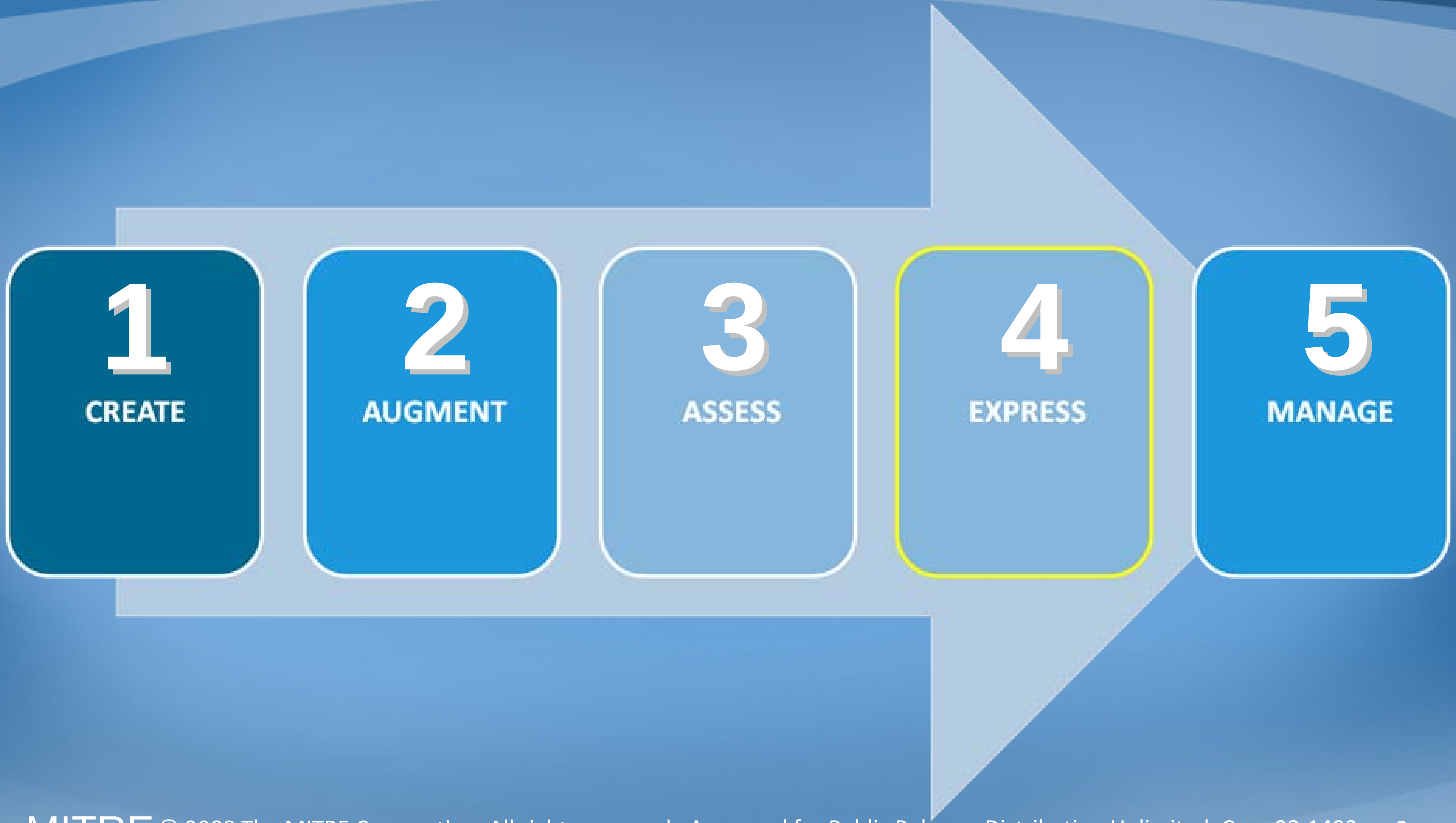
Agenda

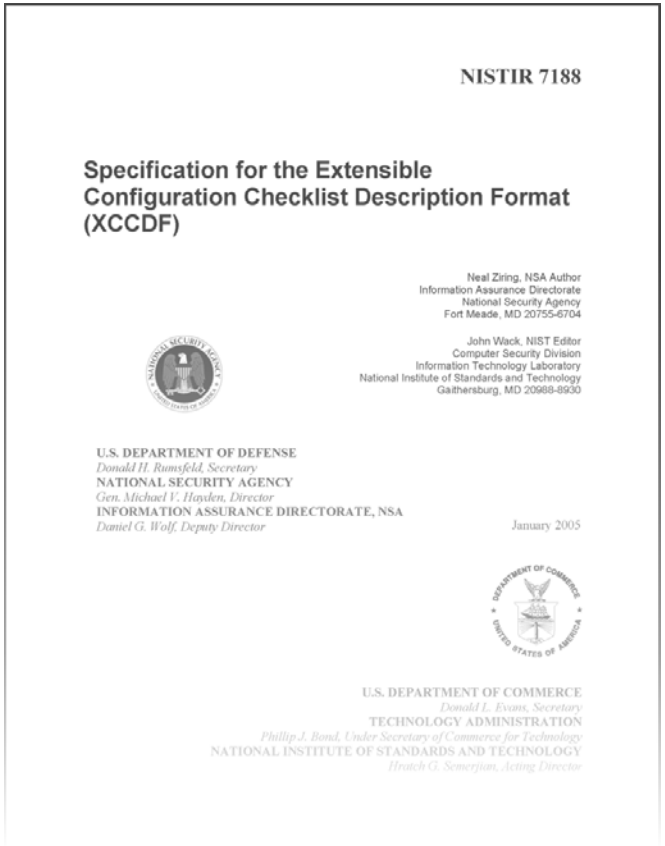
10:00-10:10	Introduction
10:10-11:15	Phase 1: Writing Good Guidance
11:15-11:25	Break
11:25-12:10	Phase 2: Augmenting Rules
12:10-12:45	Phase 3: Automating Assessment
12:45-1:30	Lunch
1:30-2:45	Phase 3, Continued: Automating Assessment
2:45-2:55	Break
2:55-3:45	Phase 4: Benchmark Structure & Tailoring
3:45-4:15	Phase 5: Manage Compliance
4:15-4:30	Wrap Up

Phase 4: Benchmark Structure & Tailoring



What is XCCDF

- **The eXtensible Configuration Checklist Description Format**
- **An XML specification for expressing security benchmarks and recording assessment results**
- **Designed for three purposes:**
  - driving system security checking tools
  - generating human-readable documents and reports
  - scoring and tracking compliance



NISTIR 7188

Specification for the Extensible Configuration Checklist Description Format (XCCDF)

Neal Ziring, NSA Author
Information Assurance Directorate
National Security Agency
Fort Meade, MD 20755-6704

John Wack, NIST Editor
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20988-8930

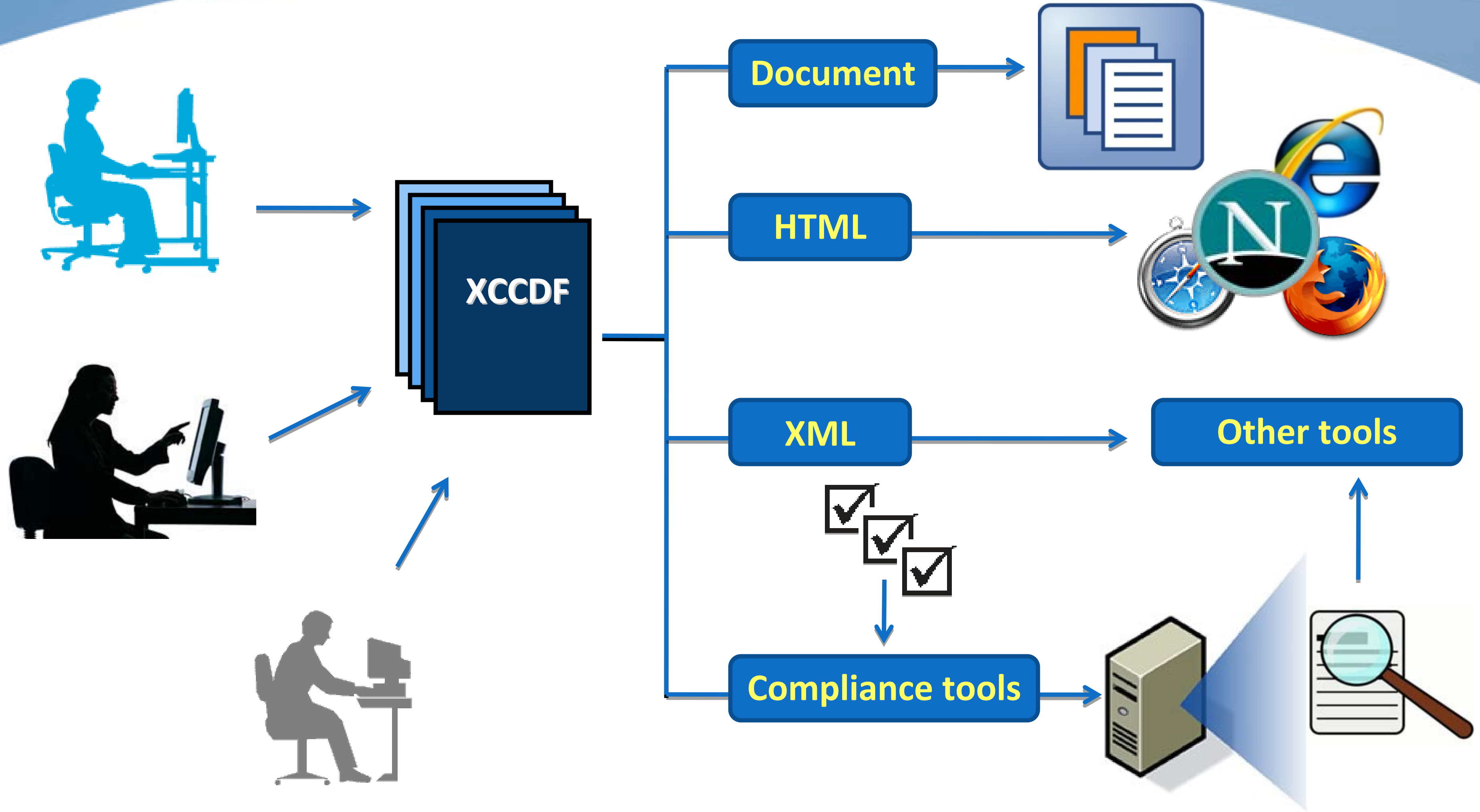
U.S. DEPARTMENT OF DEFENSE
Donald H. Rumsfeld, Secretary
NATIONAL SECURITY AGENCY
Gen. Michael V. Hayden, Director
INFORMATION ASSURANCE DIRECTORATE, NSA
Daniel G. Wolf, Deputy Director

January 2005

U.S. DEPARTMENT OF COMMERCE
Donald L. Evans, Secretary
TECHNOLOGY ADMINISTRATION
Phillip J. Bond, Under Secretary of Commerce for Technology
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Hratch G. Semerjian, Acting Director

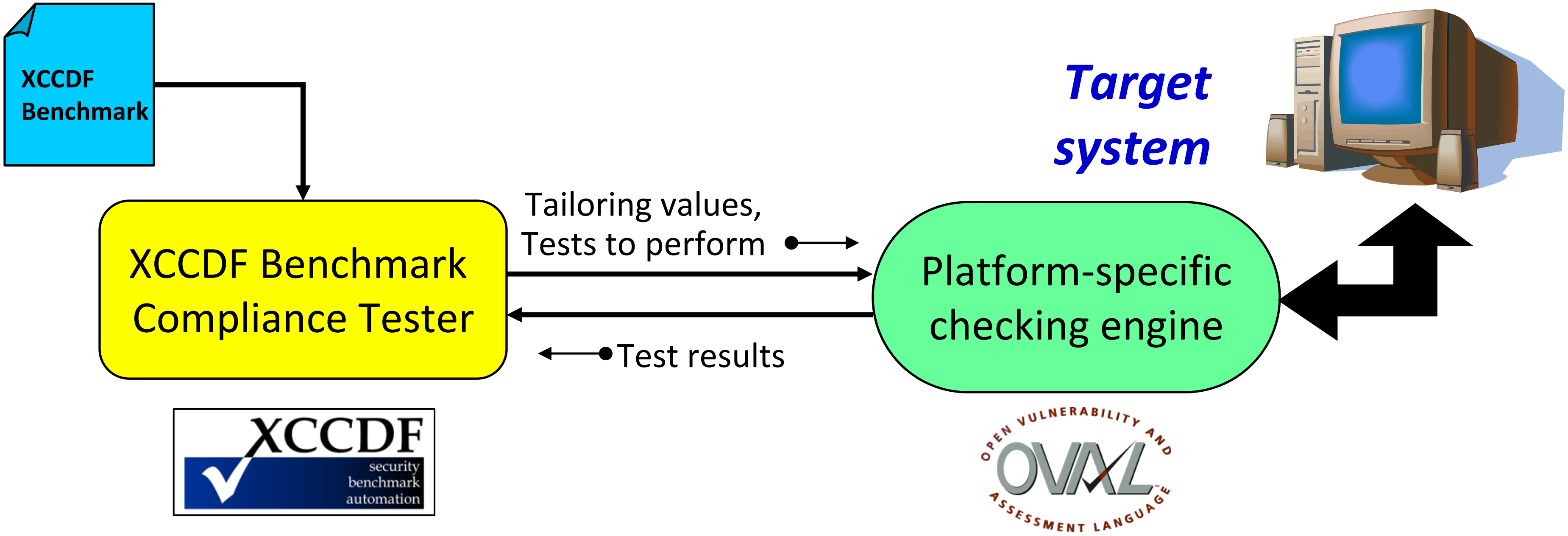
http://nvd.nist.gov/xccdf.cfm

XCCDF Use Cases

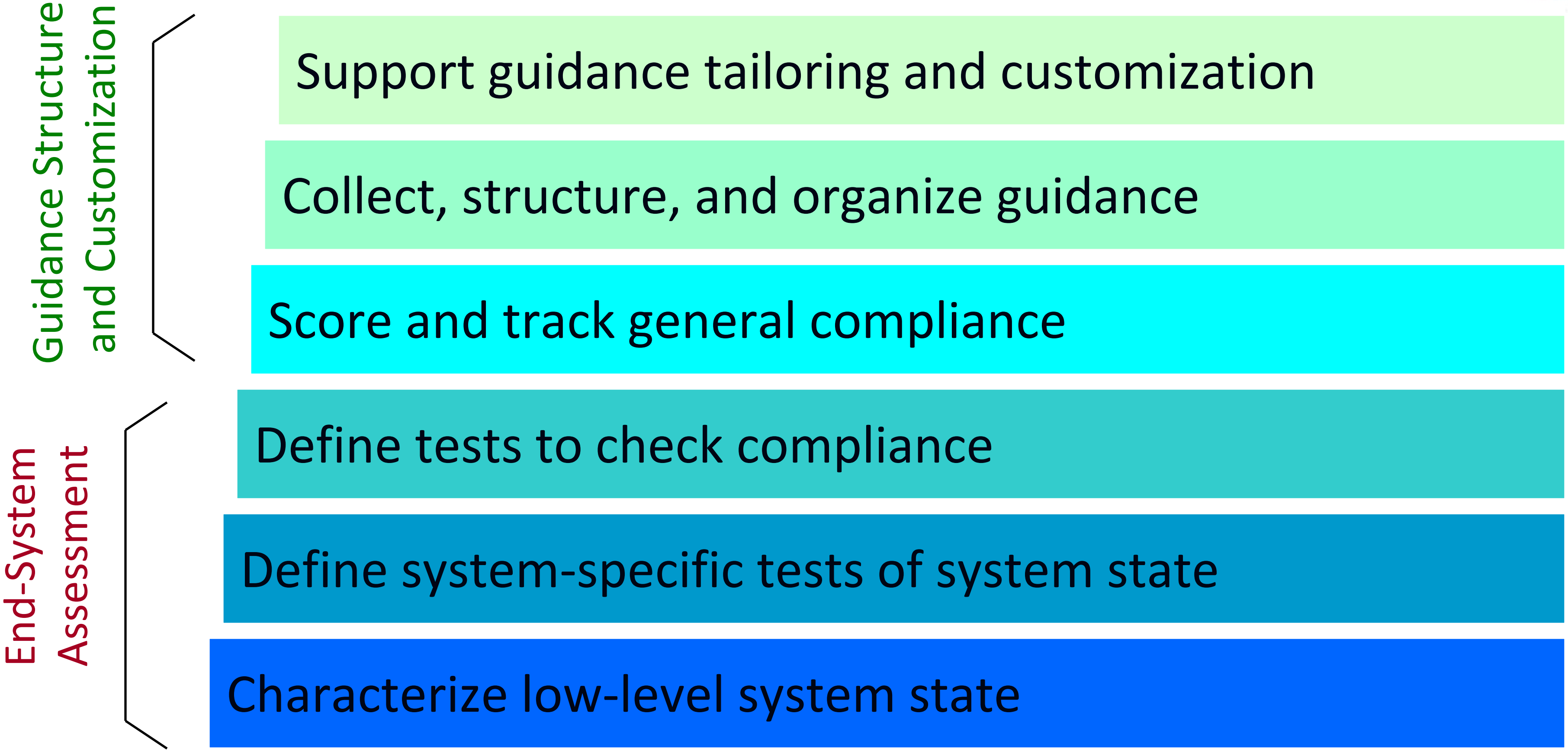


XCCDF and Checking Engines

- XCCDF does ***not*** specify platform-specific system rule checking logic.
- The `Rule/check` element contains information for driving a platform-specific checking engine.


XCCDF Benchmark
Target system
XCCDF Benchmark Compliance Tester
Tailoring values, Tests to perform
Platform-specific checking engine
Test results
XCCDF security benchmark automation
OPEN VULNERABILITY AND ASSESSMENT LANGUAGE OVAL

XCCDF and OVAL Interaction



Guidance Structure and Customization

End-System Assessment

Support guidance tailoring and customization

Collect, structure, and organize guidance

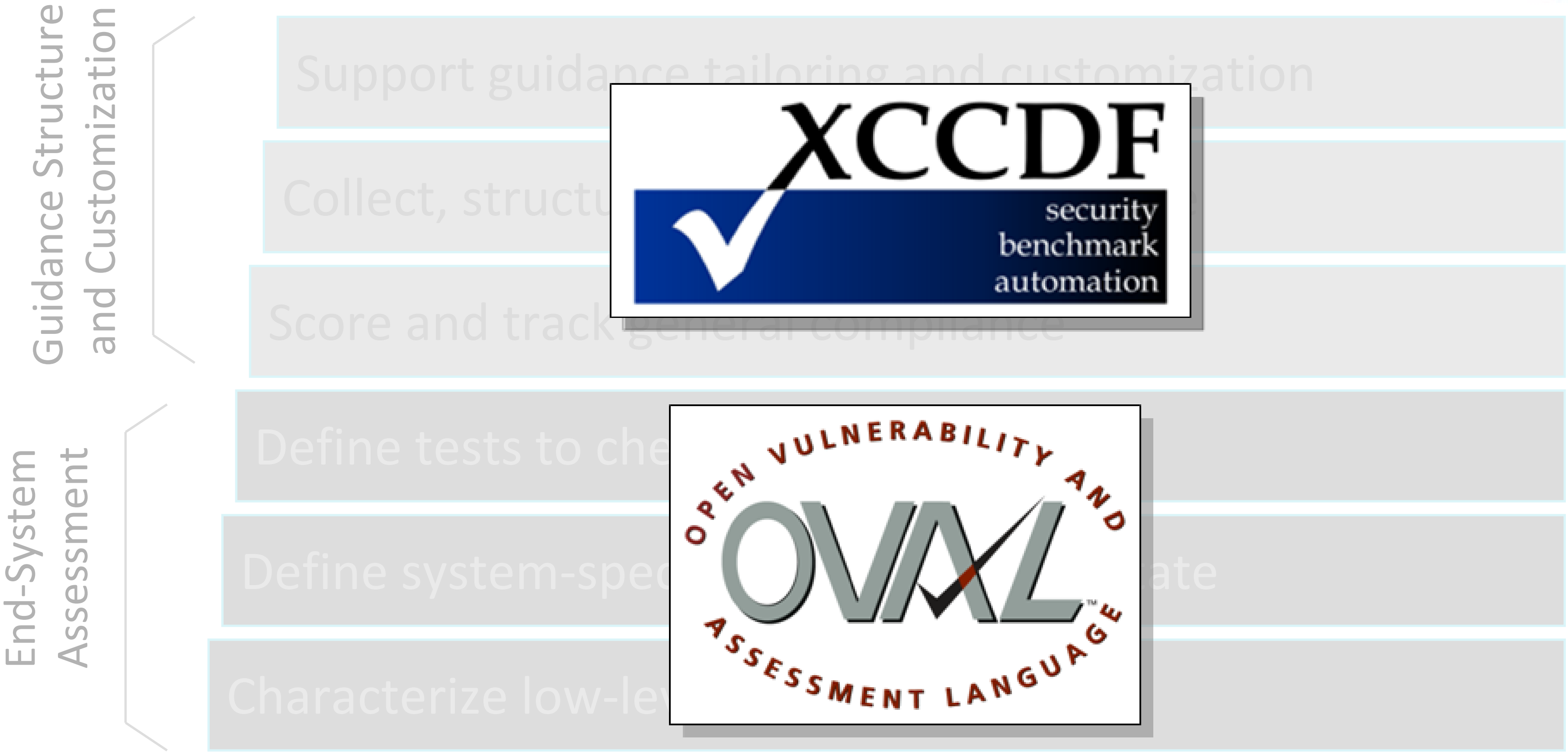
Score and track general compliance

Define tests to check compliance

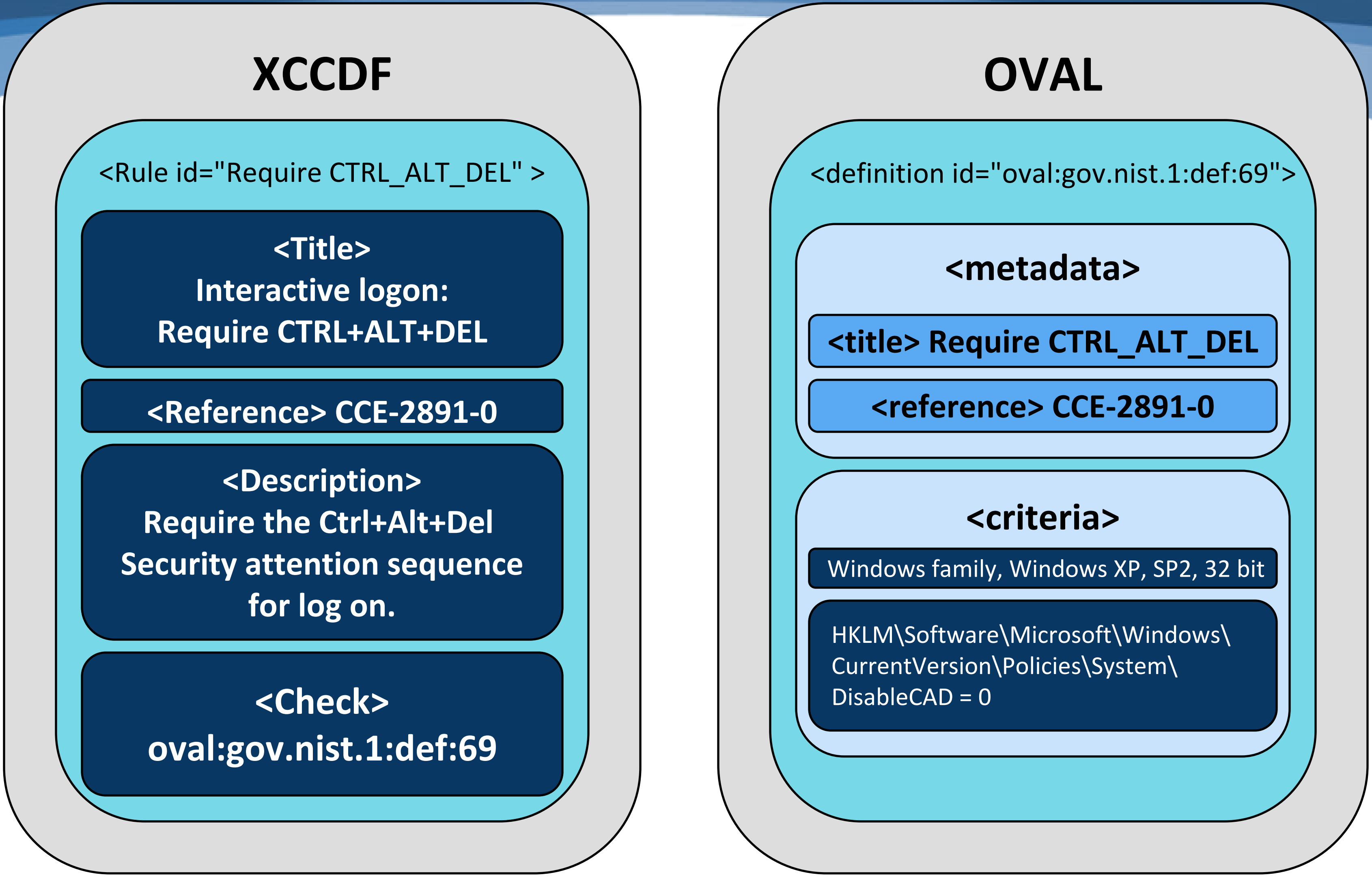
Define system-specific tests of system state

Characterize low-level system state

XCCDF and OVAL Interaction


Guidance Structure and Customization
Support guidance tailoring and customization
Collect, structu
Score and track general compliance
End-System Assessment
Define tests to che
Define system-spec
ate
Characterize low-lev
XCCDF
security benchmark automation
OPEN VULNERABILITY AND ASSESSMENT LANGUAGE
OVAL™

XCCDF & OVAL Illustrated



XCCDF

<Rule id="Require CTRL_ALT_DEL" >

<Title>
Interactive logon:
Require CTRL+ALT+DEL

<Reference> CCE-2891-0

<Description>
Require the Ctrl+Alt+Del
Security attention sequence
for log on.

<Check>
oval:gov.nist.1:def:69

OVAL

<definition id="oval:gov.nist.1:def:69">

<metadata>

<title> Require CTRL_ALT_DEL

<reference> CCE-2891-0

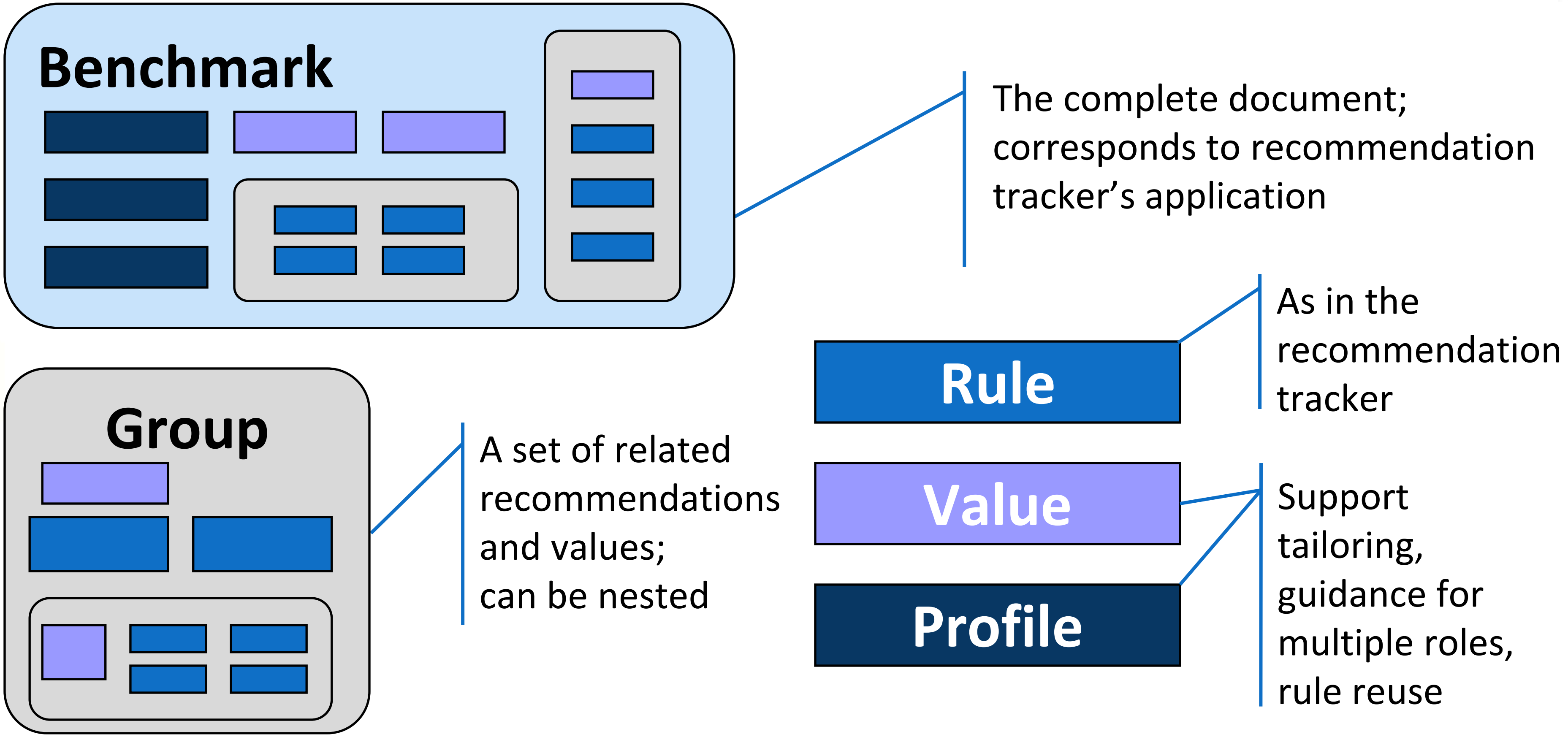
<criteria>

Windows family, Windows XP, SP2, 32 bit

HKLM\Software\Microsoft\Windows\
CurrentVersion\Policies\System\
DisableCAD = 0

XCCDF Data Model

XCCDF defines the following key object types:



Benchmark

The complete document; corresponds to recommendation tracker's application

Rule

As in the recommendation tracker

Group

A set of related recommendations and values; can be nested

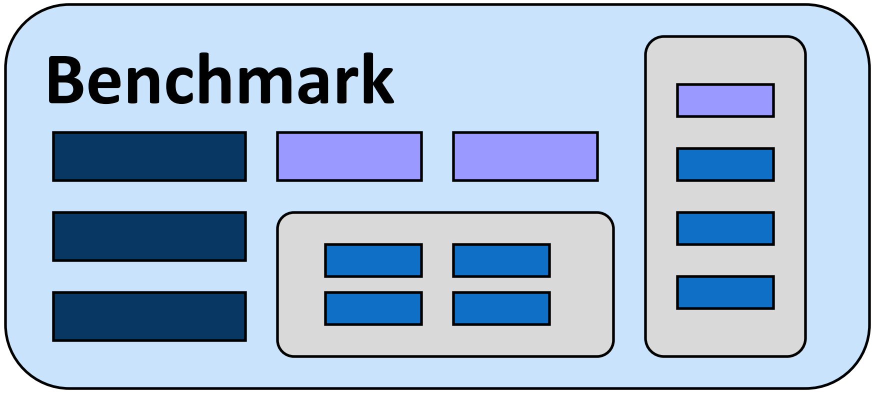
Value

Profile

Support tailoring, guidance for multiple roles, rule reuse

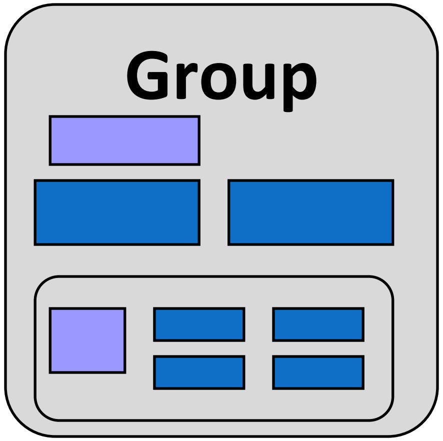
XCCDF Benchmark

```
<Benchmark id="Windows-XP">
   <title>Guidance for Securing Microsoft Windows XP</title>
   <platform idref="cpe:/o:microsoft:windows_xp"/>
   <Profile id="XP-Pro">...</Profile>
   <Group id="Chapter1">
      <Group id="PasswordPolicy">
          <Value>
          <Rule>
      </Group>
      <Group id="AuditPolicy">
           <Rule>
      </Group>
   </Group>
   <Group id="Chapter2">
   </Group>
</Benchmark>
```



XCCDF Group

```
<Group id="account_policies_group">
    <Group id="password_policies">
       <title>Password Policies</title>
       <description>In addition to educating users regarding the
      selection and use of good passwords, it is also important
      to set password parameters so that passwords are
      sufficiently strong...</description>
       <value>...</value>
       <rule>...</rule>
       <rule>...</rule>
    </Group>
</Group>
<Group id="file_permissions_group">
   ...
</Group>
```



XCCDF Rule

```
<Rule id="maximum_password_age" >
    <title>Maximum Password Age</title>
    <description>Set the “Maximum password age” password parameter to 90
   days.</description>
    <reference href="http://cce.mitre.org">CCE-2920-7</reference>
    <rationale>The “Maximum password age” password parameter is set to
         force users to change passwords at regular, defined, intervals…
    </rationale>
    <fixtext>1 - Launch the Local Security Policy editor: Start ->
         All Programs -> Administrative Tools -> Local Security Policy…
    </fixtext>
    <check system="http://oval.mitre.org/XMLSchema/oval-definitions-5">
      <check-export value-id="maximum_password_age_var"
                   export-name="oval:gov.nist.fdcc.xp:var:90"/>
      <check-content-ref href="BDC-XP-oval.xml"
                        name="oval:gov.nist.fdcc.xp:def:17"/>
    </check>
</Rule>
```

Rule

XCCDF Profile

```
<Profile id="federal_desktop_core_configuration">
    <title>Federal Desktop Core Configuration</title>
    <description>This profile represents guidance outlined in
   Federal Desktop Core Configuration settings for Desktop
   systems.</description>
    <!--Password Policy Settings-->
    <select idref="maximum_password_age" selected="true"/>
    <select idref="minimum_password_length" selected="true"/>
    <refine-value idref="maximum_password_age_var"
        selector="5184000_seconds"/>
    <refine-value idref="minimum_password_length_var"
        selector="12_characters"/>
</Profile>
```

Profile

Traditional Options for Creating and Editing Benchmark XML

- Text editor
  - No assistance
  - Thorough understanding of XML and schema needed
- General-purpose XML IDE
  - Syntax highlighting, auto-indent, element begin & end
  - Schema-aware
  - Detailed knowledge of XML and schema still required

Benchmark XML Creation and Editing Simplified

- Generate XCCDF with the Recommendation Tracker
  - All guidance for an application exportable as XCCDF
- Edit XML using the Benchmark Editor
  - Hides XML syntax
  - Provides unified view of benchmark
    - XCCDF and OVAL, and any other XML format
  - Requires greatly reduced knowledge of XML formats

Demo: Benchmark Editor Editing of XCCDF