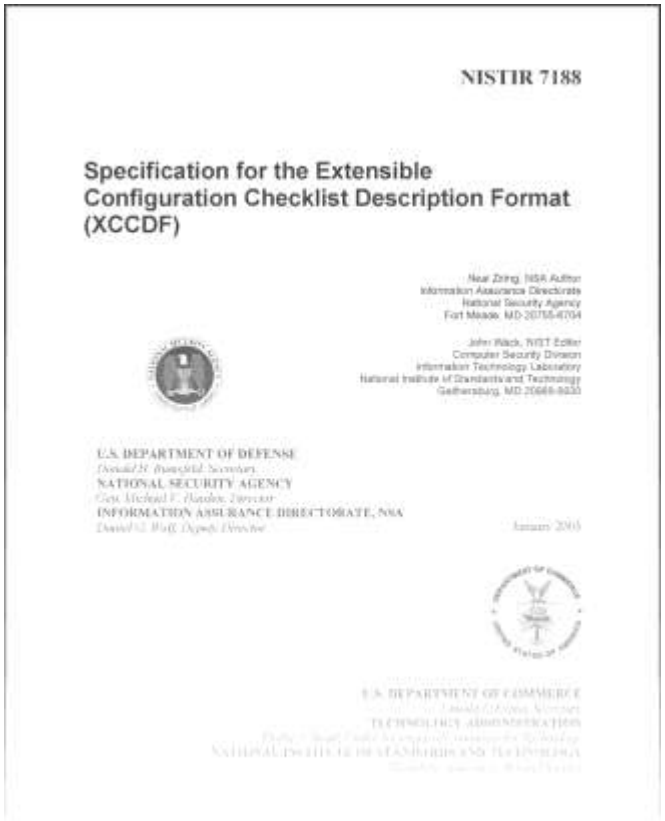
An Introduction to XCCDF

Bryan Worrell

MITRE

What is XCCDF?

- The eXtensible Configuration Checklist Description Format
- An XML specification for expressing security benchmarks and recording assessment results.
- Enables automated compliance checking
- Actively being developed
  - Current version is 1.1.4
  - Version 1.2.0 is in Draft


NISTIR 7188

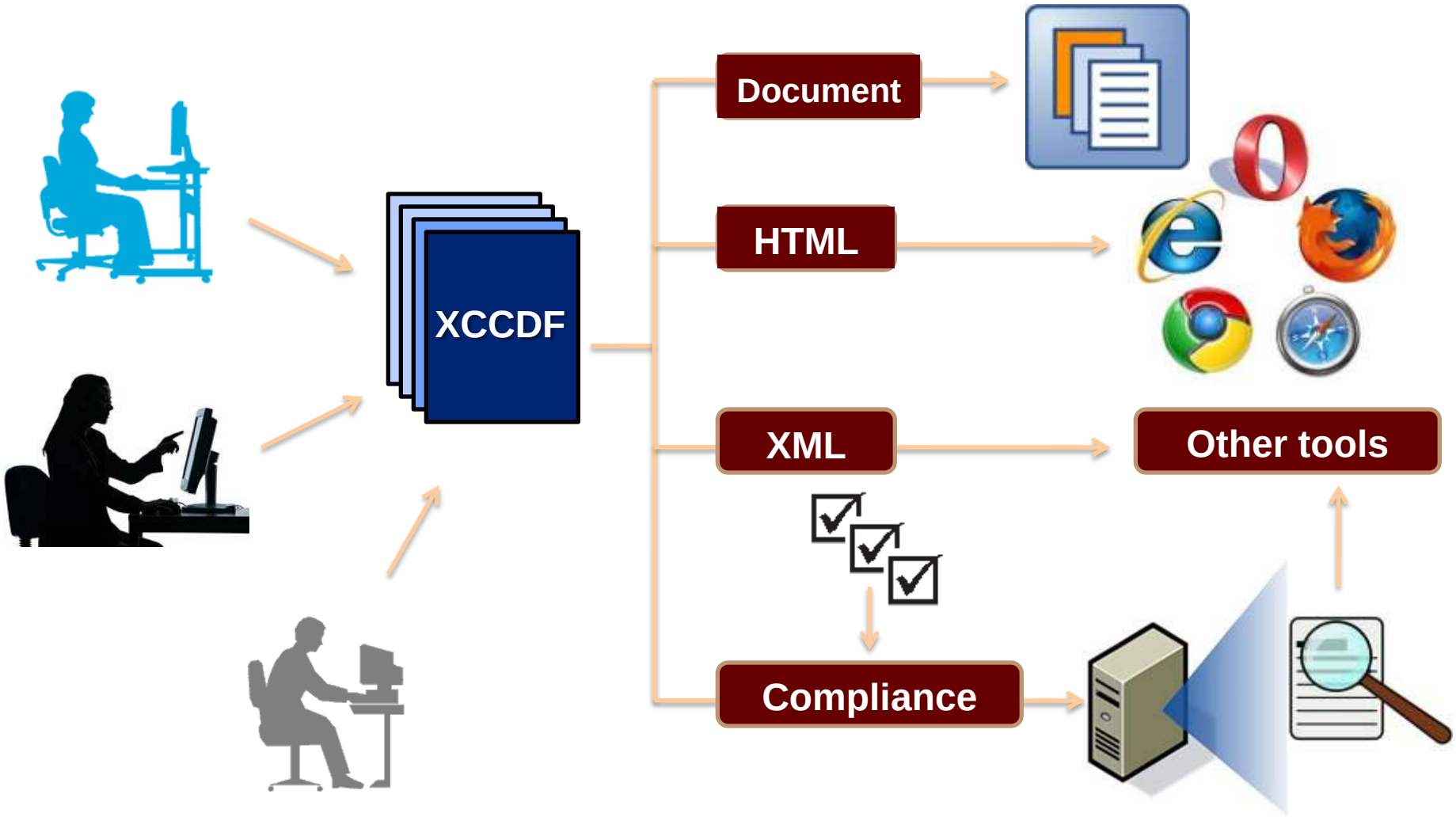
Specification for the Extensible Configuration Checklist Description Format (XCCDF)

U.S. DEPARTMENT OF DEFENSE
NATIONAL SECURITY AGENCY
INFORMATION ASSURANCE DIRECTORATE, NSA

Compliance… To Me

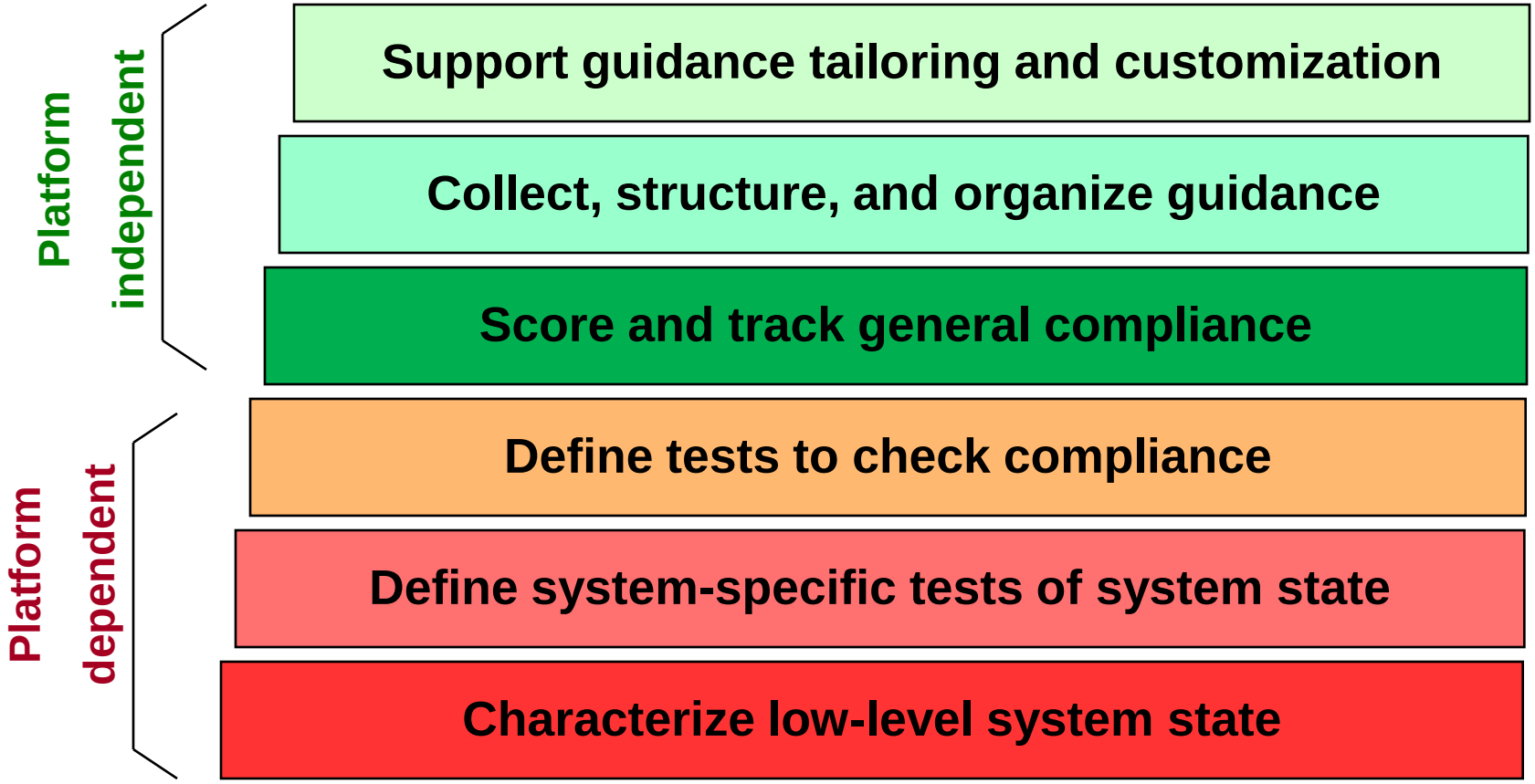
- Three pieces to compliance
  - Policy
    - A concrete portrayal (prose document) of how systems within an organization should be configured
  - Assessment
    - Determining the compliance of a system or systems within an organization as defined by the policy document
  - Remediation
    - Taking non-compliant systems and either making them compliant or filing for exemptions

XCCDF Use Cases



General Requirements

We need a language or languages to address these areas:

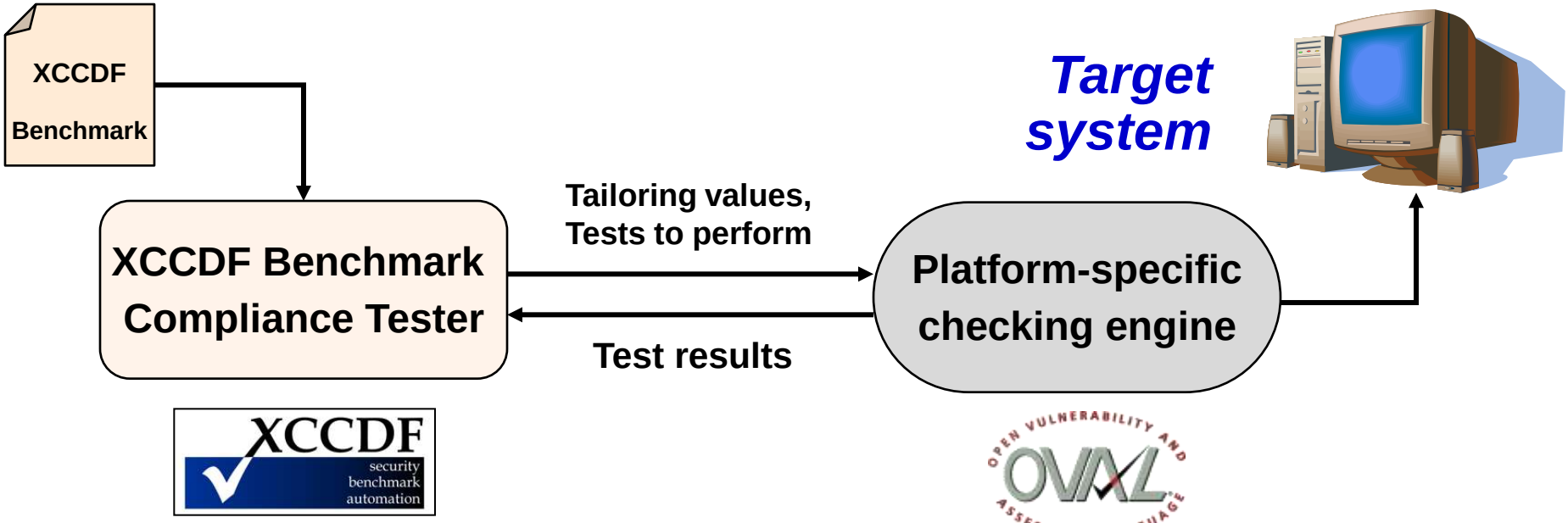


General Requirements

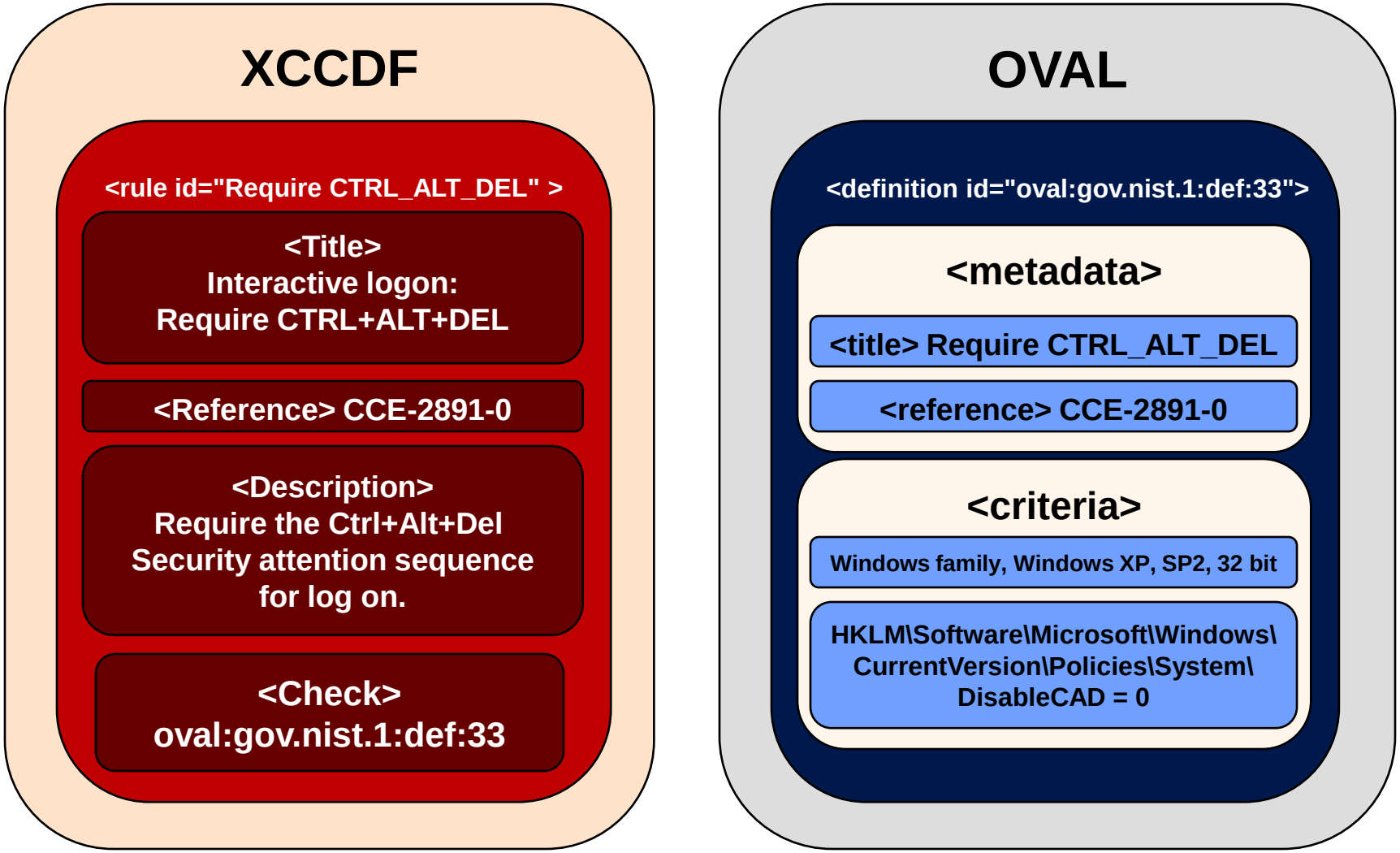
We need a language or languages to address these areas:

XCCDF and Checking Engines

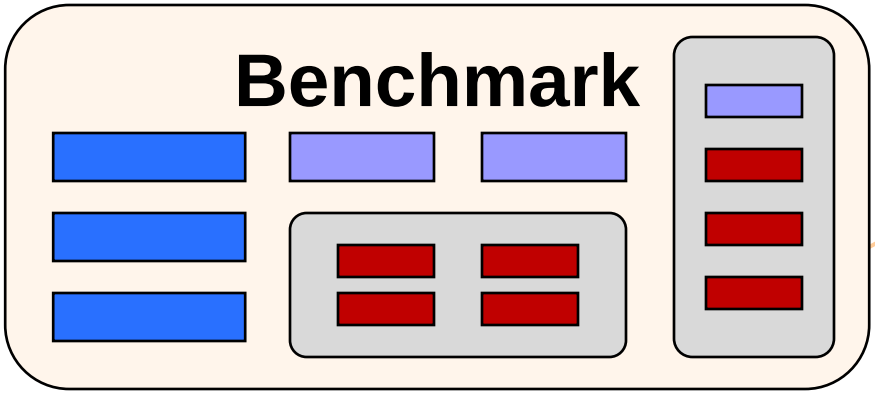
- **XCCDF does *not* specify platform-specific system rule checking logic.**
  - **The `Rule/check` element contains information for driving a platform-specific checking engine.**



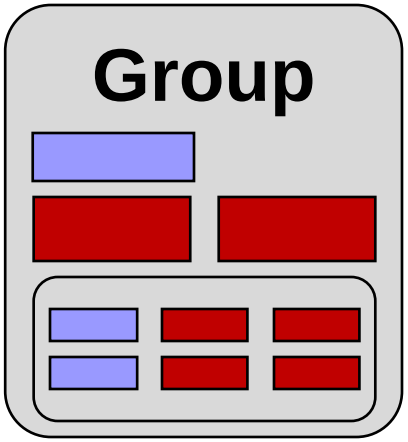
XCCDF & OVAL Illustrated



XCCDF Data Model



The complete document



A set of related recommendations and values; can be nested

Rule

Value

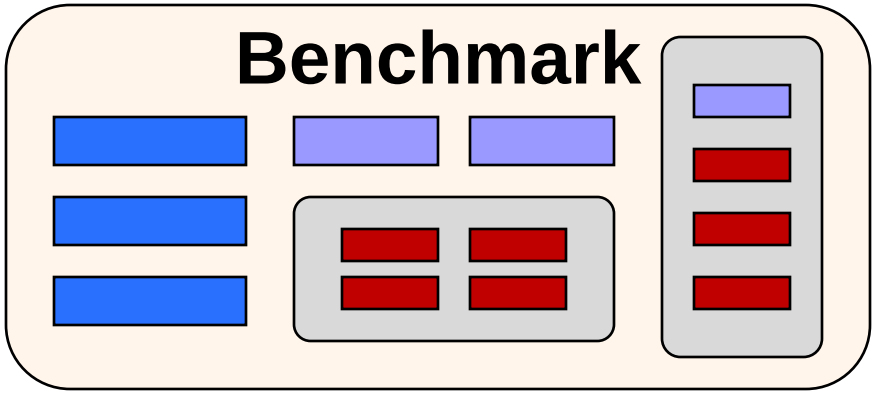
Profile

An individual recommendation

Support tailoring, guidance for multiple roles, rule reuse

XCCDF Benchmark XML

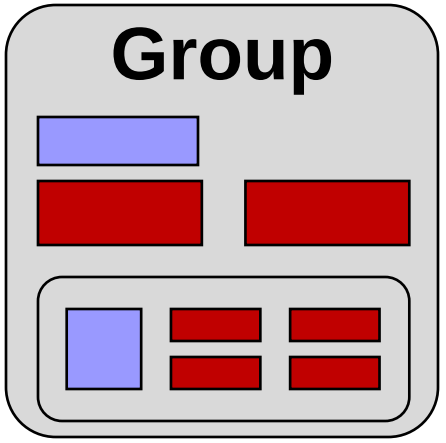
```
<Benchmark id="Windows-XP">
  <title>Guidance for Securing Microsoft Windows XP</title>
  <platform idref="cpe:/o:microsoft:windows_xp"/>
  <Profile id="XP-Pro">...</Profile>
  <Group id="Chapter1">
     <Group id="PasswordPolicy">
        <Value> ... </Value>
        <Rule>  ... </Rule>
     </Group>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



XCCDF Group XML

- Groups contain a collection of related Rules, Groups, and Values
  - In guidance or policy documents, Groups can be thought of as chapters

```
<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

- Rules define benchmark recommendations or policy statements
  - Does not define logic for implementing the rule
  - <fixtext> element provides a prose description of steps for bringing a machine into a compliance

- Can contain a reference to an automated check
  - Enables automated compliance checking for the policy statement

XCCDF Rule XML

```
<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

Selected Attribute

- Selecting a Rule or a Group tells the XCCDF processor to evalute it.
  - If a Rule or Group is NOT selected, it will not be processed

```
<Rule id="" selected="false">
   <title></title>
   <description></description>
   <reference></reference>
   <requires idref=""/>
   <check system=""></check>
</Rule>
```

- Tip: turn Rules off by default
  - Profiles can be used to turn rules on

Requires

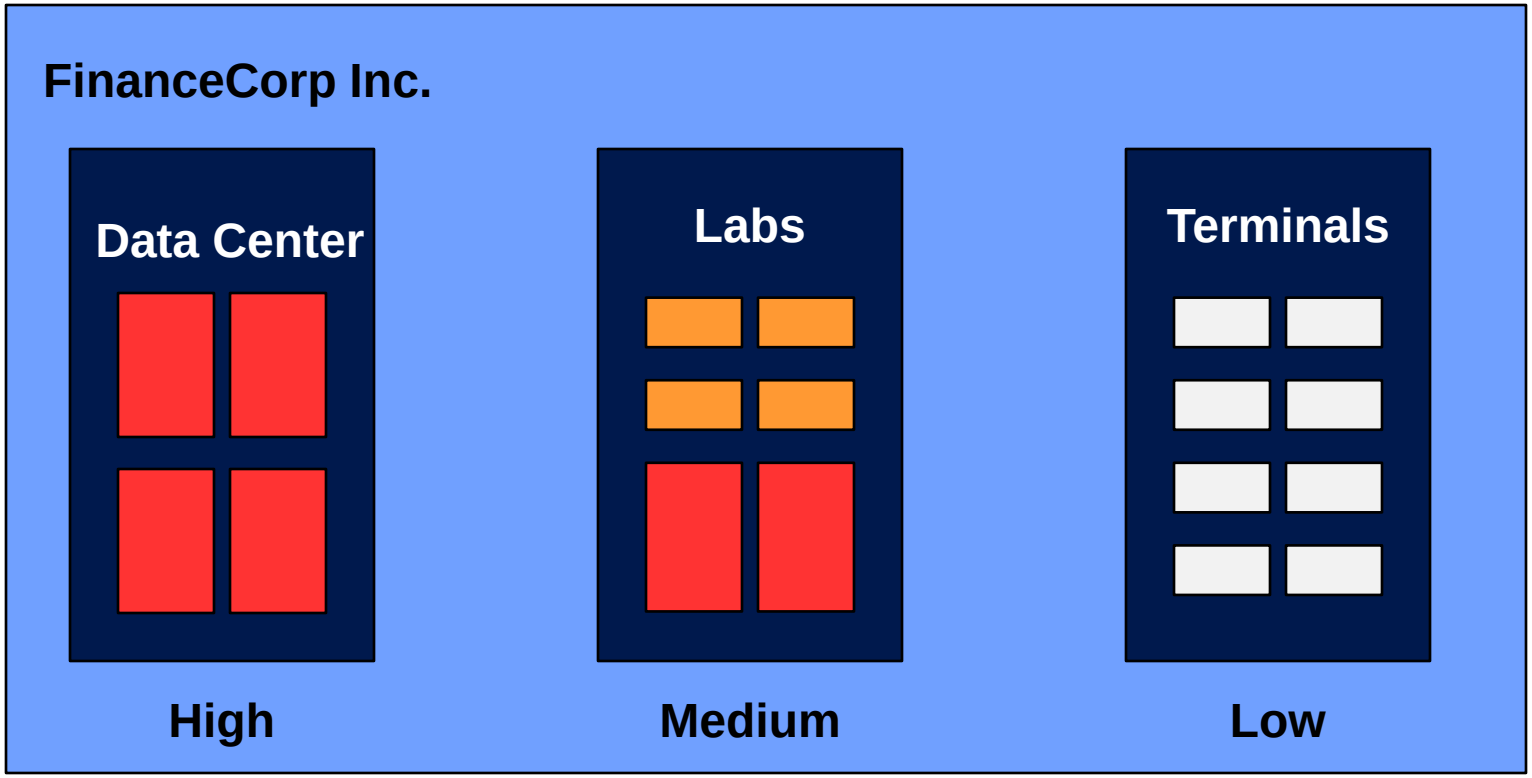
- Rule can only be selected if required Group/Rule is selected
  - ignore local selected attribute if "requires" fails

```
<Rule id="minimum_password_length" selected="true">
   <title></title>
   <description></description>
   <reference></reference>
   <requires idref="enforce_password_auth"/>
   <check system="">
      <check-export value-id="" export-name=""/>
      <check-content-ref href="" name=""/>
   </check>
</Rule>

<Rule id="enforce_password_auth">
   <title></title>
   <description></description>
   <reference></reference>
   <check system="">
      <check-export value-id="" export-name=""/>
      <check-content-ref href="" name=""/>
   </check>
</Rule>
```

Tailoring XCCDF

- XCCDF documents can be tailored to fit your organizational needs



Tailoring XCCDF

- One XCCDF Document to rule them all…
- Profiles and Values are the mechanisms
- Profiles allow you to change values (ex: password length requirements) or turn on/off rules
- Values are where you store all possible choices for a requirement
  - Password length (8, 12, 16, etc.)
  - Account lockout threshold (3 attempts? 50 attempts?)
  - Password expiration (1 week? 3 months?)

XCCDF Value

- A tailoring mechanism, used for storing variables
  - Passed along to checking engines
  - Value determined at runtime after Profile processing

```
<Value id="account_lockout_threshold" type="number" operator="less than or
  equal">
  <title>Account Lockout Threshold</title>
  <description>The maximum number of failed attempts that can occur before
  the account is locked out</description>
  <default>50</default>
  <value selector="3_attempts">3</value>
  <value selector="10_attempts">10</value>
  <value selector="50_attempts">50</value>
</Value>

<Rule id="account_lockout" selected="true">
  <title></title>
  <description></description>
  <check system="oval5">
      <check-export value-id="account_lockout_threshold" name="oval:var:1"/>
      <check-content-ref href="oval-def.xml" name=""/>
  </check>
</Rule>
```

XCCDF Profile

- Tailoring module for XCCDF Benchmarks
- Turn on/off Rules
- Choose what values to use
- Benchmarks can contain multiple Profiles
  - Profile is chosen to be applied at runtime

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

Refined Values

```
<Value id="value-x" type="" operator="">
   <default>1</default>
   <value selector="AA">2</value>
   <value selector="BB">3</value>
</Value>

<Profile id="ONE">
   <title></title>
   <description></description>
   <refine-value idref="value-x" selector="AA"/>
</Profile>

<Rule id="accounts" selected="true">
   <title></title>
   <description></description>
   <check system="oval">
      <check-export value-id="value-x" export-name=""/>
      <check-content-ref href="oval-def.xml" name=""/>
   </check>
</Rule>
```

Inheritance

- Profiles, Groups, Values, and Rules all contain an "extends" attribute.

- Inheritance allows us to establish a parent-child relationship
  - Children receive values from their parents
  - Enables code reuse
  - One change to a parent updates all extending children

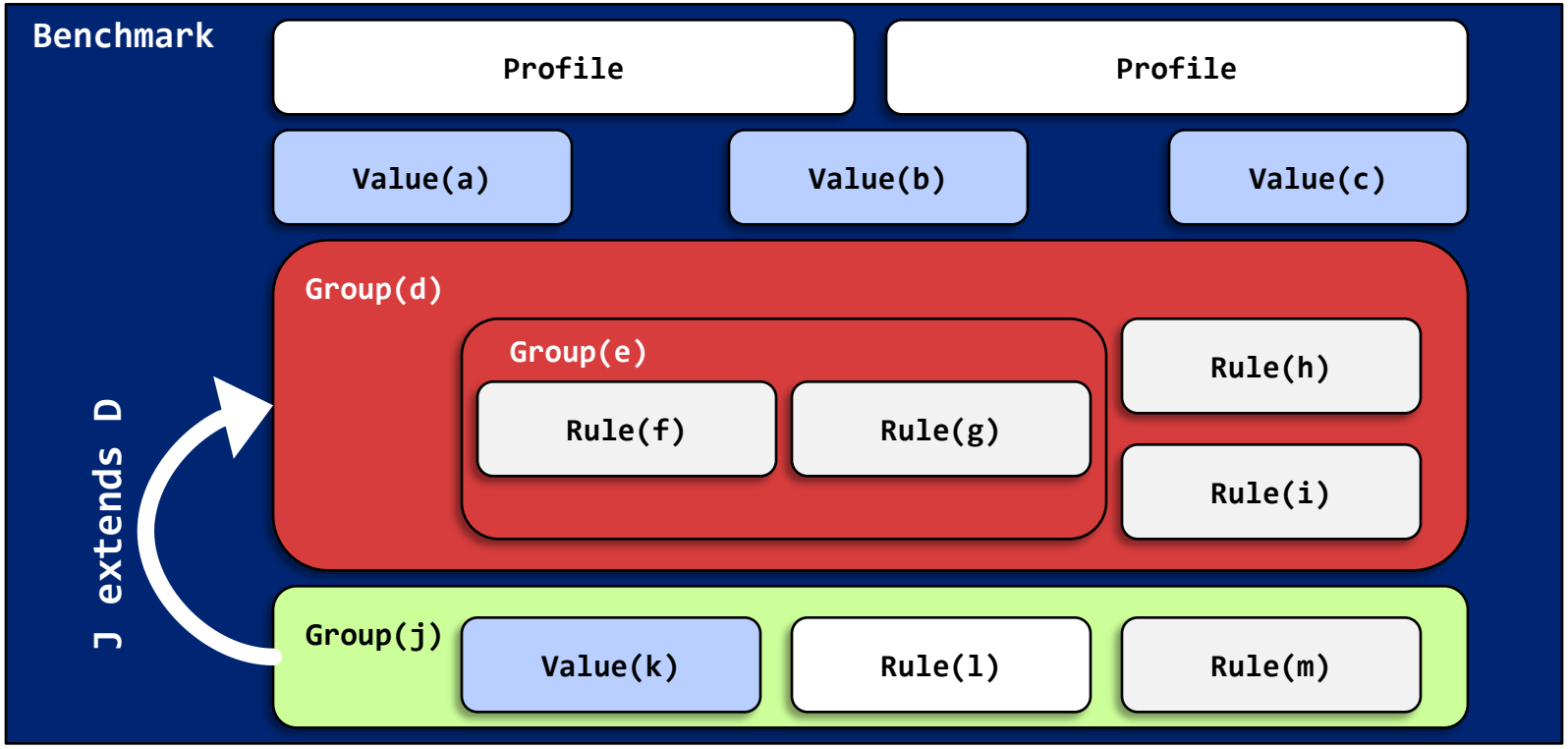
- Inheritance can get a little tricky…

Inheritance Processing

- None
  - The property value or values are not inherited.
- Prepend
  - The property values are inherited from the extended object, but values on the extending object come first, and inherited values follow.
- Append
  - The property values are inherited from the extended object; additional values may be defined on the extending object.
- Replace
  - The property value is inherited; a property value explicitly defined on the extending object replaces an inherited value.
- Override
  - The property values are inherited from the extended object; additional values may be defined on the extending object.

Inheritance and Scoping

- Item Y can extend Item X if they are the same type and one of the following…
  - X is a direct child of the Benchmark
  - X is a direct child of a Group which is also an ancestor of Y
  - X is a direct child of a Group which is extended by an ancestor of Y



XCCDF Results

- XCCDF Results provide a structured language for representing compliance assessment results
- Results can be consumed by tools for further analysis, report generation, or remediation
- Contain the following information
  - The guidance document/checklist with tailoring applied
  - Information about the target system and architecture
  - The time interval of the assessment and times of each rule invokation
  - Compliance scores
  - References to lower level details possibly stored in output files

SCAP Data Streams

- NCP (National Checklist Program)
  - http://web.nvd.nist.gov/view/ncp/repository
- FDCC (Federal Desktop Core Configuration)
  - http://nvd.nist.gov/fdcc
- USGCB (United States Government Configuration Baseline)
  - http://usgcb.nist.gov

Open Source Tools: Authoring

- **Benchmark Editor**
  - Developed at The MITRE Corporation
  - Focuses on developing and editing benchmark documents written in standardized languages such as XCCDF and OVAL
  - http://sourceforge.net/projects/benchmarkeditor/
- **eSCAPe**
  - Developed at G2 Inc.
  - Focuses on the development of SCAP content
  - http://www.g2-inc.com/escape
- **Recommendation Tracker**
  - Developed at The MITRE Corporation
  - Focuses on the development of security guidance, utilizing SCAP standards
  - http://sourceforge.net/projects/rectracker

Open Source Tools: Assessment

- OpenSCAP
  - http://www.open-scap.org/
  - Linux library for working with SCAP standards
- XCCDF Reference Implementation
  - http://scap.nist.gov/specifications/xccdf/
  - Developed by NIST and MITRE
  - Binary distribution packaged with open source checking engines
    - OVAL Interpreter
    - OCIL Interpreter

Community

- XCCDF is a community driven project
  - Get Involved!
- Automation Track - XCCDF
  - Charles Schmidt discussing XCCDF
- Mailing list
  - xccdf-dev@nist.gov
  - Archive at http://n2.nabble.com/XCCDF-f1363789.html
- Website
  - http://scap.nist.gov/specifications/xccdf/

Questions?