



Automated Audit of Compliance and Security Controls

Gerhard Koschorreck
g.koschorreck@upw.de
UPW ProjectServices GmbH

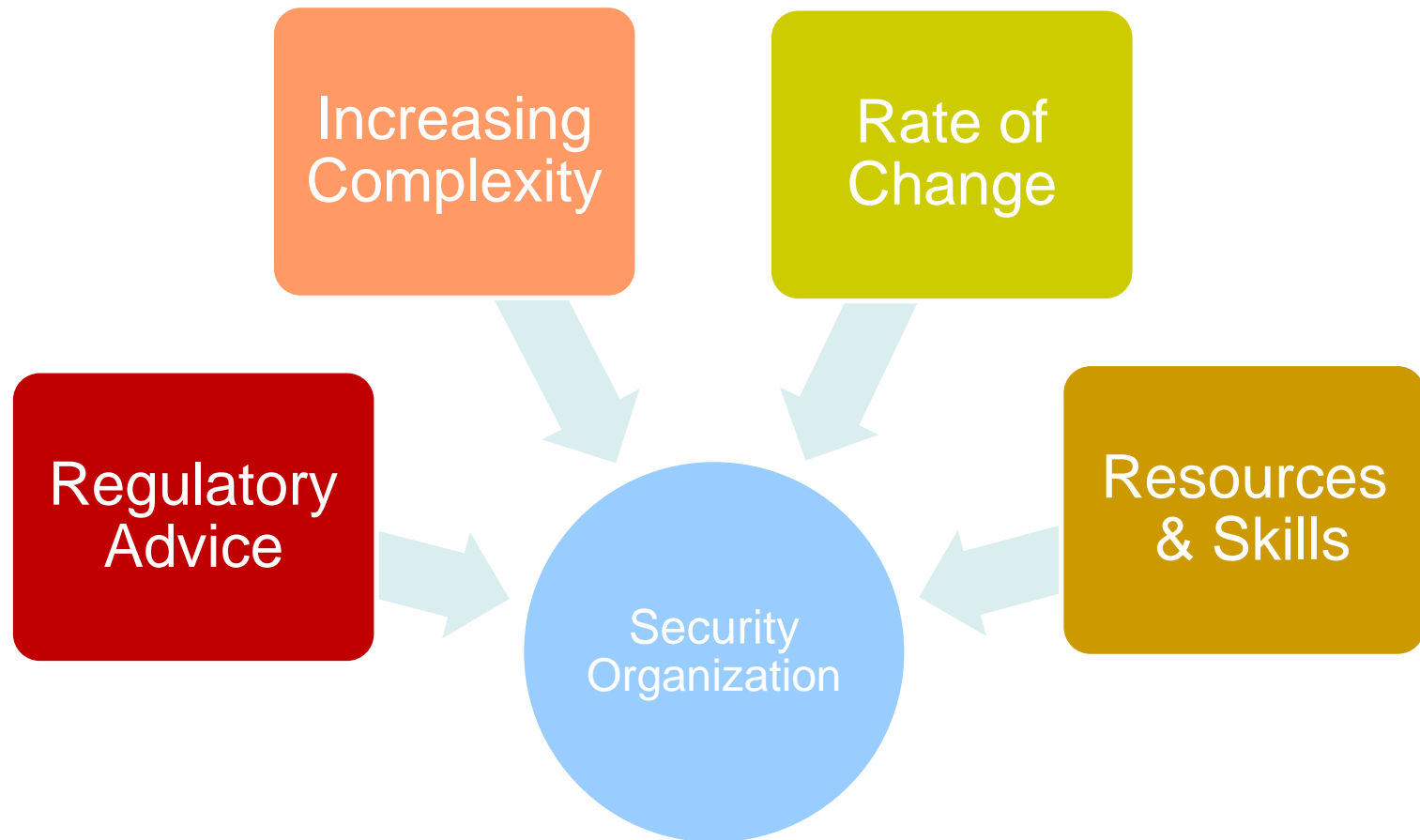


AGENDA

1	Information Security Challenges
2	Solutions
3	Types Of Controls
4	OVAL: A Closer Look
5	XCCDF
6	Conclusions



Challenges





Regulatory Advice (US & International)

Public Company Accounting
Oversight Board (PCAOB)

Federal Information Security
Management Act (FISMA)

Payment Card Industry Data
Security Standard (PCI DSS)

Sarbanes-Oxley Act (SOX)

Financial Services
Modernization Act

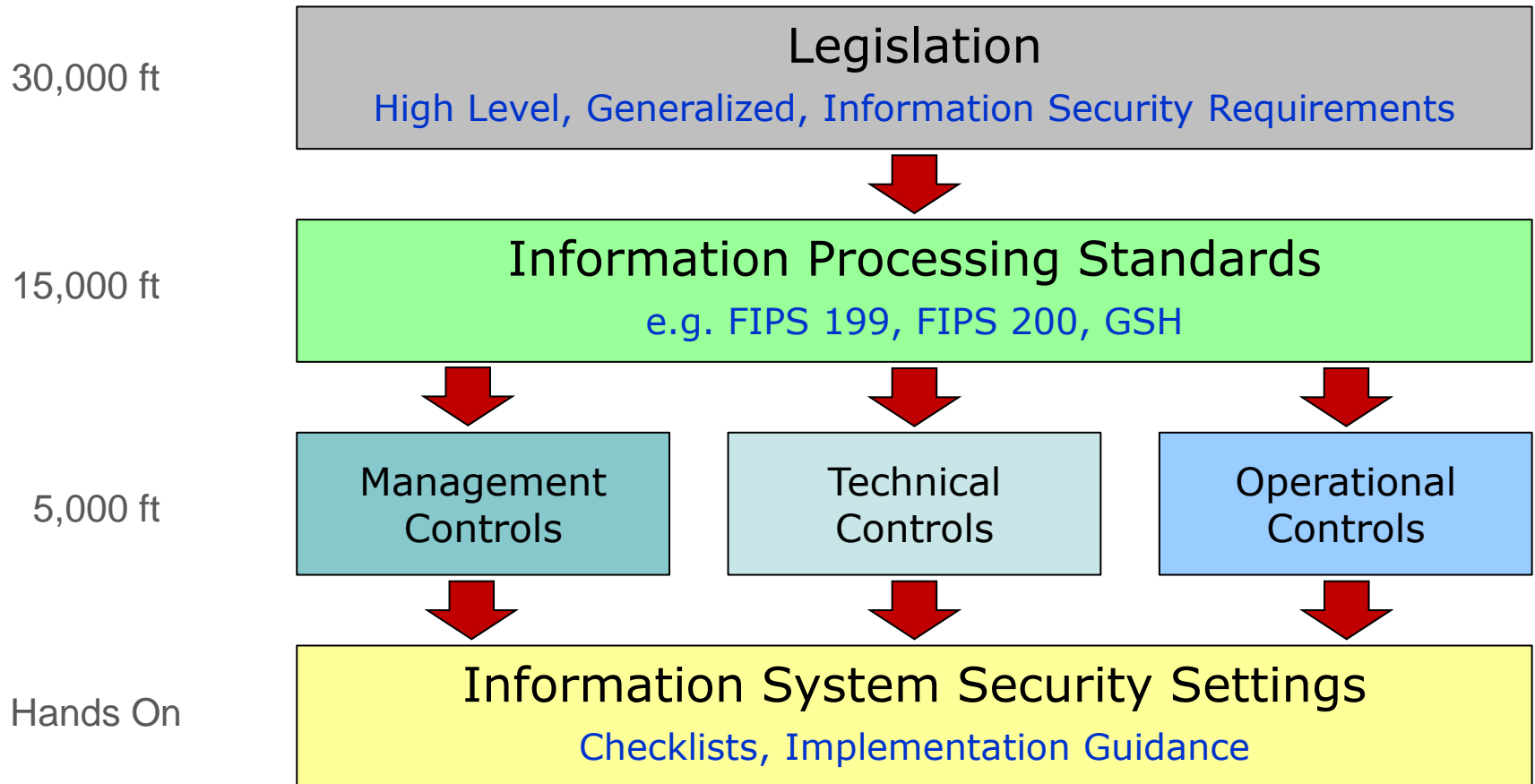
Control Objectives for
Information and Related
Technology (CobiT)

Information Technology
Infrastructure Library (ITIL)

International Standards
Organization ISO 2700x



Compliance Model





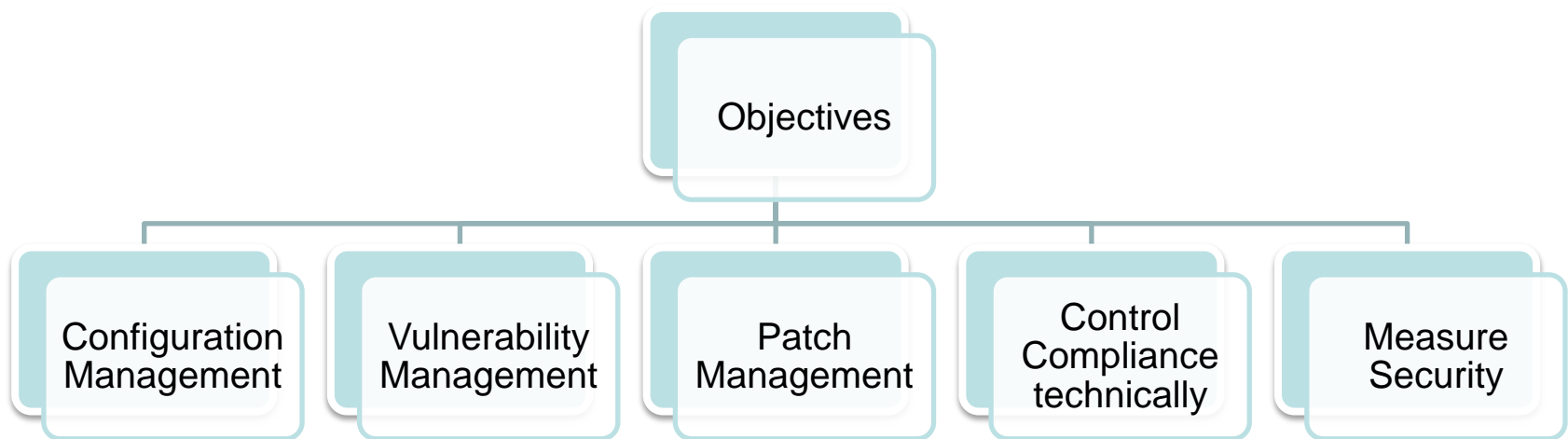
AGENDA

1	Information Security Challenges
2	Solutions
3	Types Of Controls
4	OVAL: A Closer Look
5	XCCDF
6	Conclusions



Initiatives to Automate Security

- *Making Security Measurable*
MITRE Corporation
- *Security Content Automation Protocol (SCAP)*
National Institute of Standards and Technology (NIST)





Building Blocks of Security Automation

Identify objects uniquely

Define rules

Collect guidance in
repositories



Identify Objects Uniquely

- **CVE** Common **Vulnerability** Enumeration
- **CWE** Common **Weakness** Enumeration
- **CCE** Common **Configuration** Enumeration
- **CPE** Common **Platform** Enumeration
- **CAPEC** Common **Attack Pattern** Enumeration and Classification
- **MAEC** **Malware** Attribute Enumeration and Characterization





Define Rules

- **OVAL** Open *Vulnerability* and *Assessment* Language
- **XCCDF** eXtensible *Checklist* Configuration Description Format
- **OCIL** Open Checklist *Interactive* Language
- **CVSS** Common *Vulnerability Scoring* System
- **OCRL** Open Checklist *Reporting* Language





Repositories

- OVAL Repository
- National Vulnerability Database (NVD)
- NIST: Security Content Automation Protocol (SCAP)
- National Checklist Program Repository
- Vendors: Microsoft, Red Hat, Novell, Debian
- United States Government Configuration Baseline (USGCB)

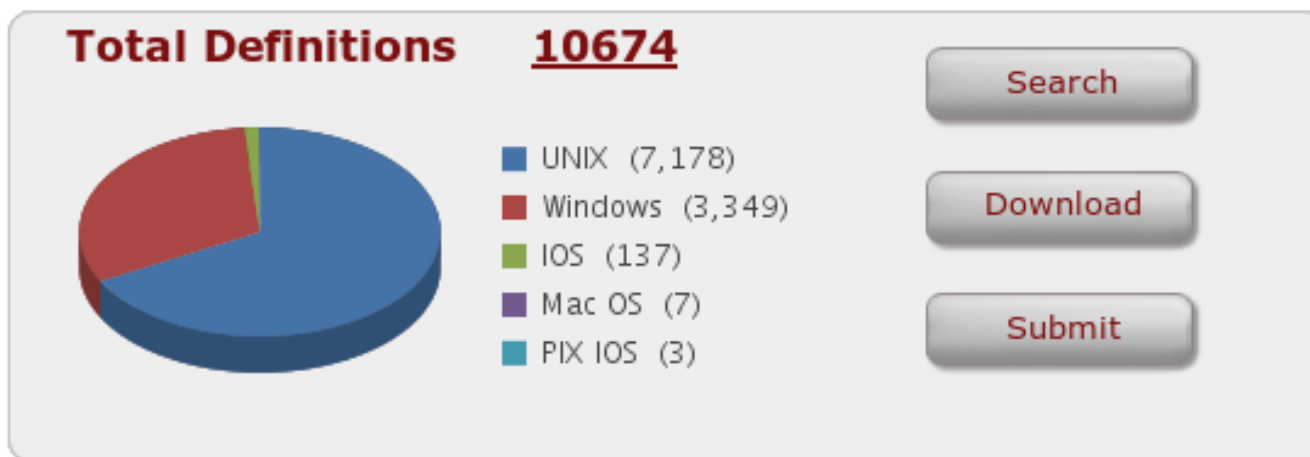




OVAL Repository

Last Repository Update: May 03, 2011 04:36 AM

The OVAL Repository is the central meeting place for the [OVAL Community](#) to discuss, analyze, store, and disseminate [OVAL Definitions](#). Members of the community contribute definitions by posting them to the [OVAL Repository Forum](#), where the OVAL Team and other members of the community review and discuss them.



The OVAL Repository contains all community-developed OVAL Vulnerability, Compliance, Inventory, and Patch Definitions for supported operating systems. Definitions are free to use and implement in information security products and services.



The Security Content Automation Protocol (SCAP)

Areas addressed

- Automated configuration
- Vulnerability checking
- Patch checking
- Technical control of compliance activities
- Security measurement

SCAP makes use of:

XCCDF, OVAL, OCIL, CPE, CCE, CVE, and CVSS



AGENDA

1	Information Security Challenges
2	Solutions
3	Types Of Controls
4	OVAL: A Closer Look
5	XCCDF
6	Conclusions

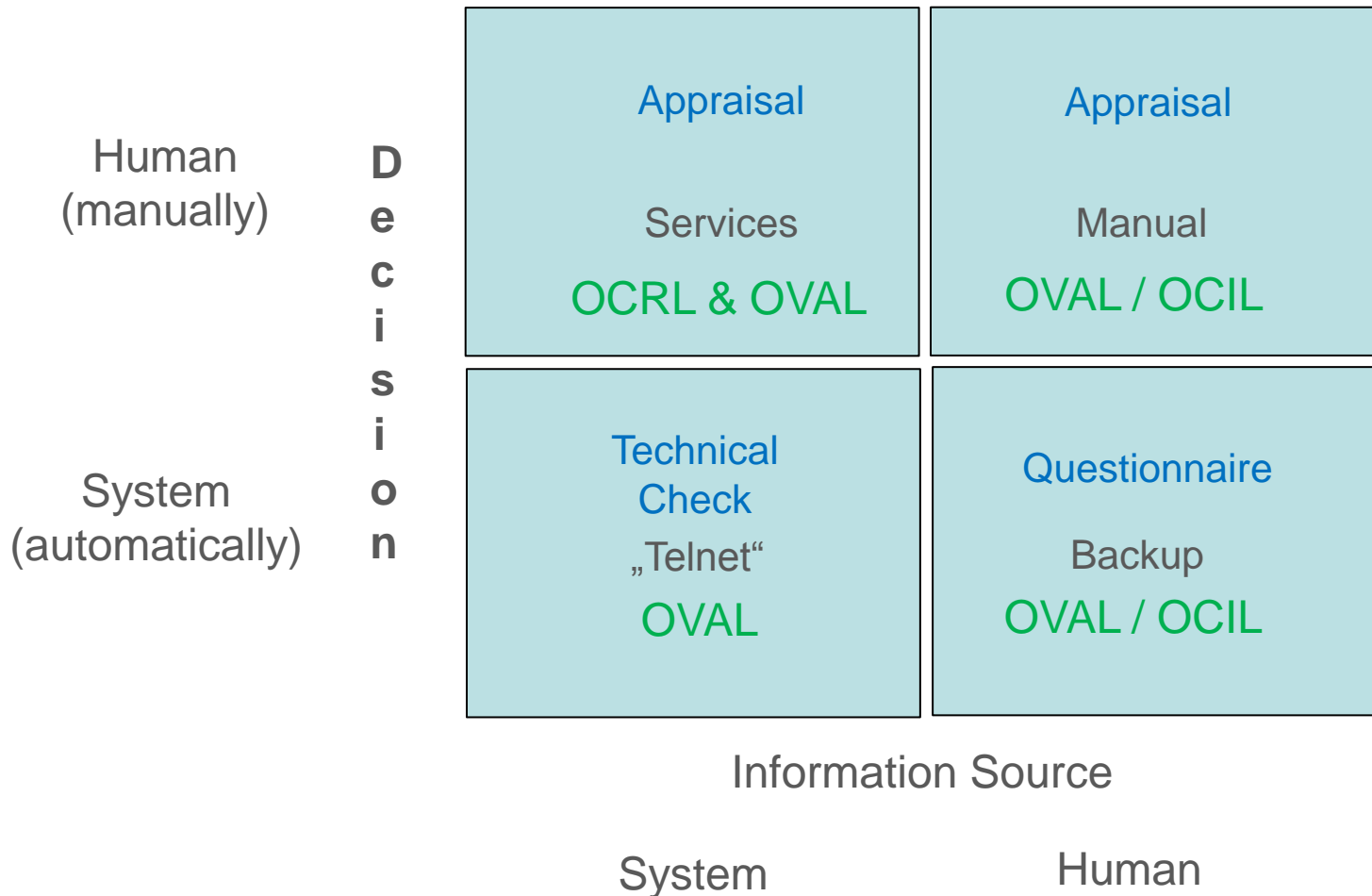


Example Controls

- “Telnet has to be deactivated”
- “Undesired services should be disabled”
- “Backup procedure should be tested twice a year”
- “There should exist a reviewed emergency manual”

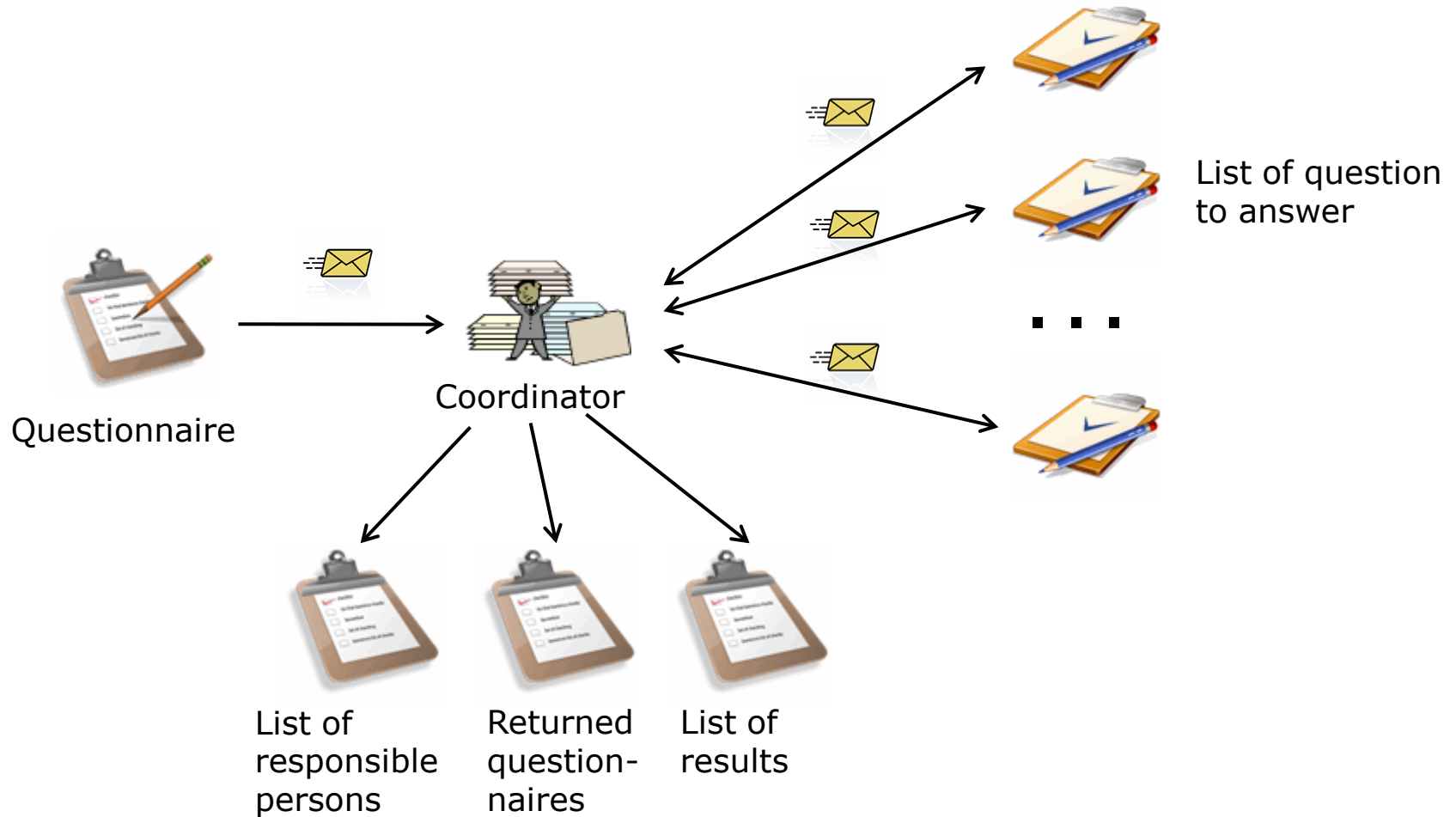


Types of Controls



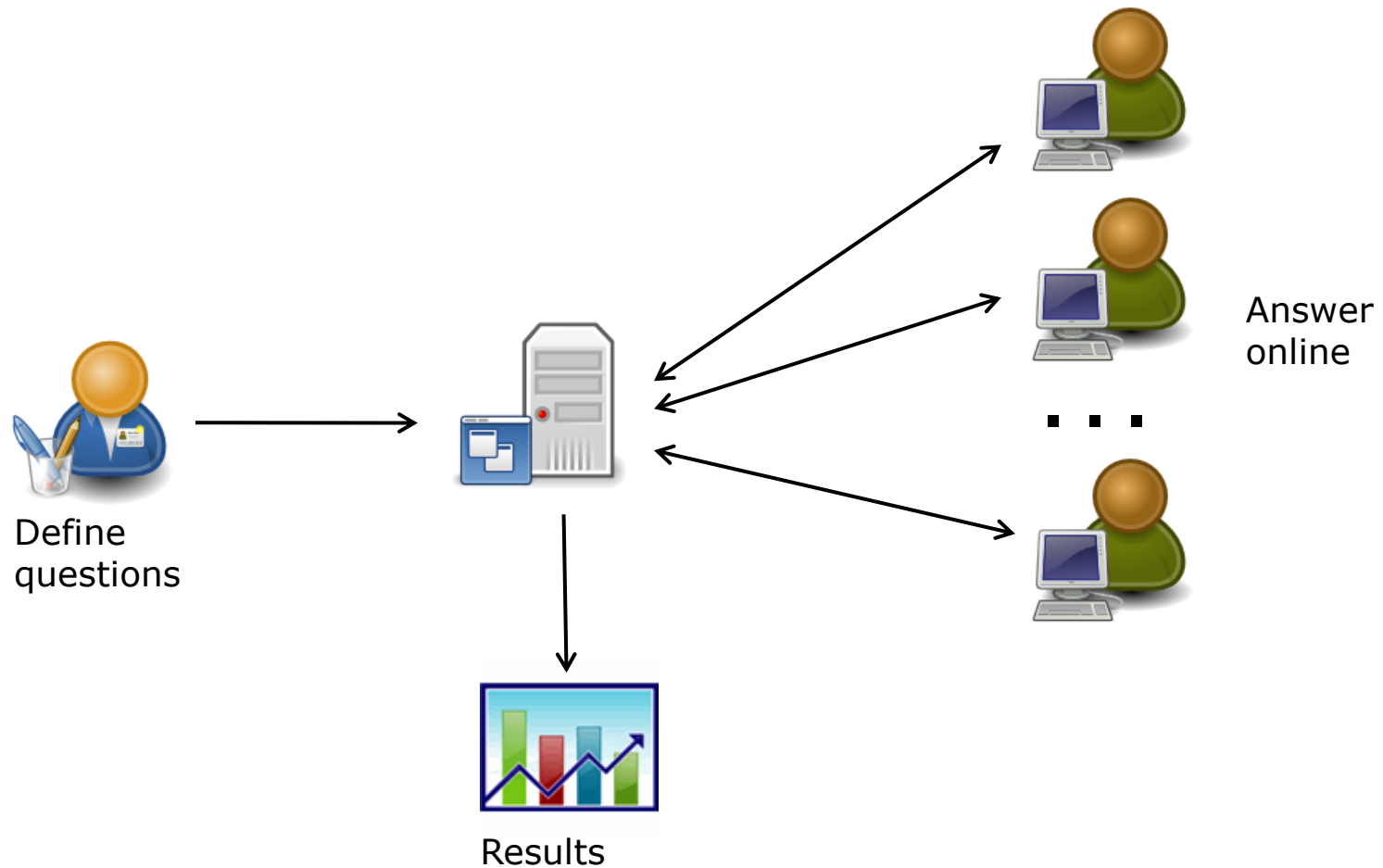


"Classical" Compliance Self Assessment





Tool-based Self Assessment

















Rendering OVAL Definitions as Web Page

PCI-DSS Requirement 02@Koschorreck, Gerhard (g.koschorreck)

Sort by

	07/04/2011 g.koschorreck	PCI-DSS 2.2.1: Is only one primary function per server implemented?	<input type="radio"/> Yes <input type="radio"/> No	 	<input type="checkbox"/>
	07/04/2011 g.koschorreck	PCI-DSS 2.2.2: Are all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the device's specified function) disabled?	<input type="radio"/> Yes <input type="radio"/> No	 	<input type="checkbox"/>
	07/04/2011 g.koschorreck	PCI-DSS 2.2.3.a: Have system administrators and/or security managers knowledge of common security parameter settings for system components?	<input type="radio"/> Yes <input type="radio"/> No	 	<input type="checkbox"/>
	07/04/2011 g.koschorreck	PCI-DSS 2.2.3.b: Are common security parameter settings included in the system configuration standards?	<input type="radio"/> Yes <input type="radio"/> No	 	<input type="checkbox"/>



AGENDA

1	Information Security Challenges
2	Solutions
3	Types Of Controls
4	OVAL: A Closer Look
5	XCCDF
6	Conclusions



Structure of an OVAL Document

```
<?xml version="1.0" encoding="utf-8"?>  
<oval_definitions ... >
```

<pre><generator> ... </generator></pre>
<pre><definitions> ... </definitions></pre>
<pre><tests> .. </tests></pre>
<pre><objects> .. </objects></pre>
<pre><states> ... </states></pre>
<pre><variables> ... </variables></pre>

```
</oval_definitions>
```



OVAL Objects (Examples)

general

- Environment Variable
- File Hash
- File Content

Solaris

- ISA
- Package
- Patch
- SMF

Unix gen.

- User
- File
- Interface
- Runlevel
- Uname
- (x)inetd
- Process

Linux

- Package
- Network

Windows

- Registry
- Passwordpolicy
- Lockoutpolicy
- Auditeventpolicy
- File
- Fileeffectiverights
- User
- WMI

Oracle

- Parameter
- Tablespace
- DB Link
- User
- Procedure



Compliance Requirement (NSA Security Guide Windows XP)

	A	B	D	E	G
1	Policy Path	Policy Setting Name	FDCC Windows XP	CCE Reference	Description
14	Computer Configuration\Windows Settings\Security Settings\Account Policies>Password Policy	Password must meet complexity requirement	Enabled	CCE-633	<p>This security setting determines whether passwords must meet complexity requirements. If this policy is enabled, passwords must meet the following minimum requirements:</p> <ul style="list-style-type: none"> • Not contain the user's account name or parts of the user's full name that exceed two consecutive characters • Be at least six characters in length <p>Contain characters from three of the following four categories:</p> <ul style="list-style-type: none"> • English uppercase characters (A through Z) • English lowercase characters (a through z) • Base 10 digits (0 through 9) • Non-alphabetic characters (for example, !, \$, #, %) <p>• Complexity requirements are enforced when passwords are changed or created.</p> <p>Default: Enabled on domain controllers. Disabled on stand-alone servers.</p> <p>Note: By default, member computers follow the configuration of their domain controllers.</p> <p>Determines whether passwords must meet complexity requirements.</p>



Corresponding OVAL Definition

```
<definition id="oval:gov.nist.fdcc.xp:def:21"
  version="1" class="compliance">
  <metadata>
    <title>Password Complexity Requirements</title>
    <affected family="windows">
      <platform>Microsoft windows XP</platform>
    </affected>
    <reference source="http://cce.mitre.org" ref_id="CCE-2735-9"/>
    <reference source="cce.mitre.org/version/4" ref_id="CCE-633"/>
    <description>Passwords must meet complexity
      requirements</description>
  </metadata>
  <criteria>
    <extend_definition comment="Microsoft windows XP is installed"
      definition_ref="oval:gov.nist.fdcc.xp:def:2"/>
    <criterion comment="Passwords must meet complexity requirements"
      test_ref="oval:gov.nist.fdcc.xp:tst:17"/>
  </criteria>
</definition>
```




Defining a Test

```
<passwordpolicy_test
  xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"
  id="oval:gov.nist.fdcc.xp:tst:17"
  version="1"
  comment="Passwords must meet complexity requirements"
  check_existence="at_least_one_exists"
  check="all">
  <object object_ref="oval:gov.nist.fdcc.xp:obj:8"/>
  <state state_ref="oval:gov.nist.fdcc.xp:ste:22"/>
</passwordpolicy_test>
```

- Tests refer to an object
- States are optional; it is possible to define several states



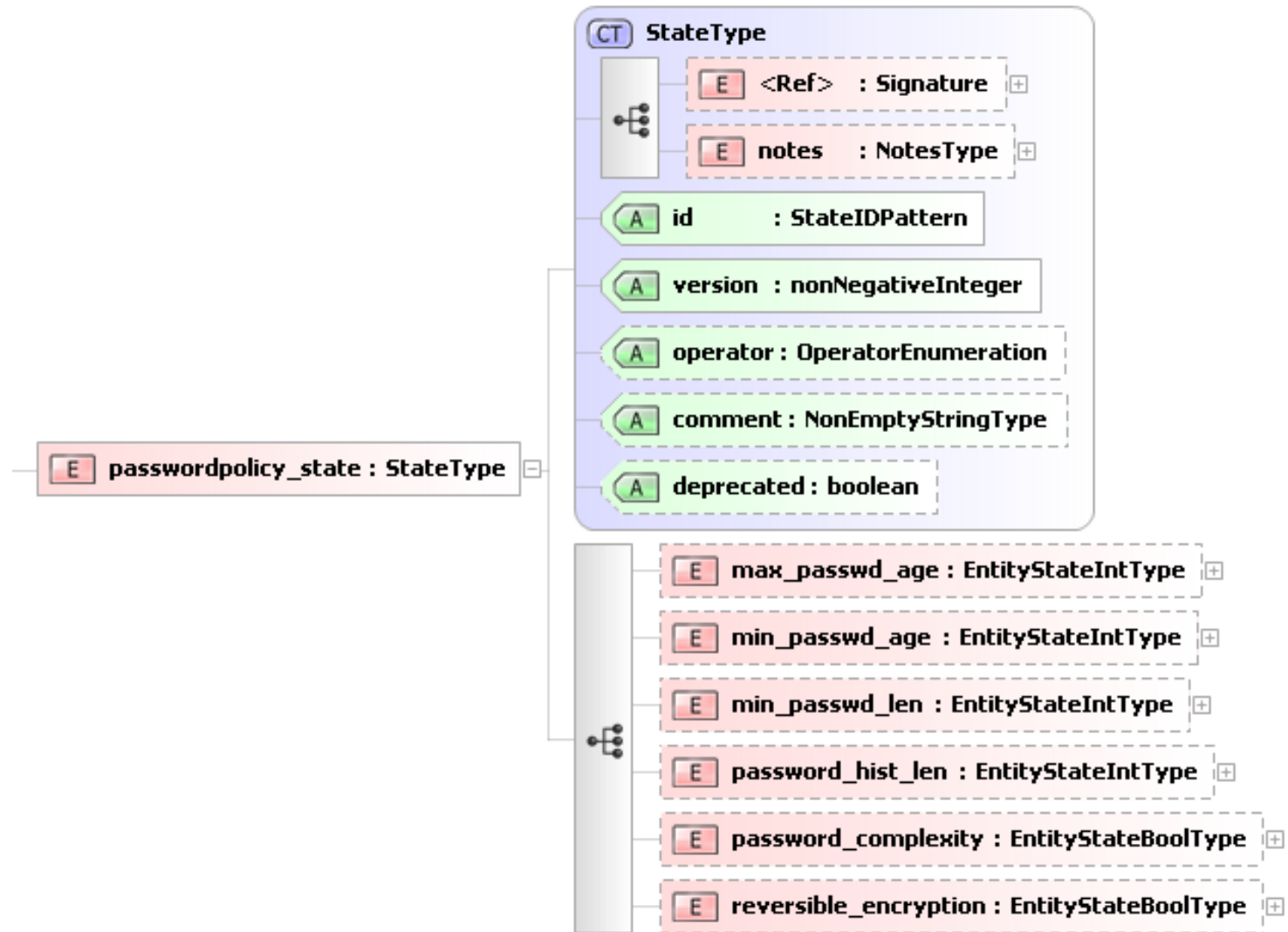
Adding an Object and a State

```
<passwordpolicy_object  
  xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"  
  id="oval:gov.nist.fdcc.xp:obj:8"  
  version="1"/>  
  
<passwordpolicy_state  
  xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"  
  id="oval:gov.nist.fdcc.xp:ste:22"  
  version="1">  
  <password_complexity  
    datatype="boolean">true</password_complexity>  
</passwordpolicy_state>
```

- States define the desired properties of the object



Details of the passwordpolicy_state



Results of an Automated Check

English (US) ▼

Welcome! You are logged in as g.koschorreck.

Logout

UPW Compliance Guard



Results

Dashboard | Keychain | Environments | Definition Sets | Jobs | Results | Reports | Survey
Editor | Survey | Survey Reports | User Preferences

Systems

Filter: hudson (1)

By Definition Set By Environment

- ☐ Network DDE DDE Share Database
- ☐ Network Dynamic Data Exchange (D
- ☐ NoDefaultExempt for IPSEC Filtering
- ☐ Offer Remote Assistance [1]
- ☐ Password Change Prompt before E
- ☒ Password Complexity Requirements
- ☐ Passwords Stored Using Reversible
- ☐ Routing and Remote Access Service
- ☐ RPC Endpoint Mapper Client Authen
- ☐ Secure Channel Data Always Digital
- ☐ Secure Channel Data Digitally Encry
- ☐ Secure Channel Data Digitally Signe

Password Complexity Requirements

AND

Password Complexity Requirements

Passwords must meet complexity requirements

Microsoft Windows XP is installed

Close



UPW
project.services

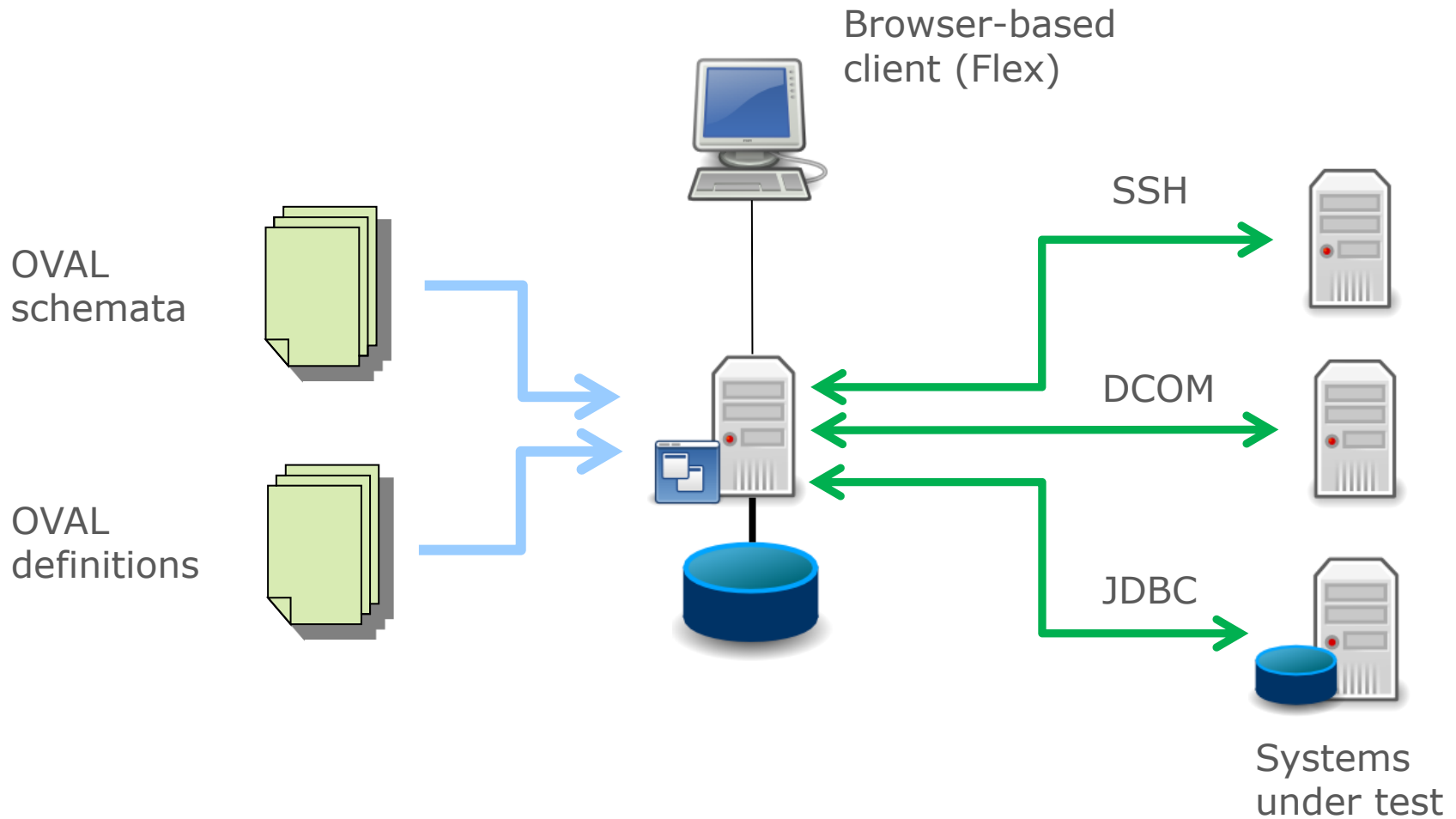


OVAL Use Cases

- Security advisory distribution
- Vulnerability assessment
- Malware detection
- Patch management
- Configuration management
- Auditing and centralized audit validation
- Security information management system (SIMS)
- System inventory



UPW Compliance Guard





Checking for Vulnerability CVE-2010-3962

Results

Dashboard | Keychain | Environments | Definition Sets | Jobs | Results | Reports | Survey Editor
| Survey | Survey Reports | User Preferences

Systems ☐ (5)

Filter: (5)

By Definition Set By Environment

- ▶ CVE-2010-0491
- ▶ CVE-2010-2729
- ▶ CVE-2010-2738
- ▶ CVE-2010-3137
- ▼ CVE-2010-3962
 - ▶ windows:admin:hudson-slave
 - ▼ windows:admin:virtual2
 - ▼ 12/21/2010 03:11 PM (23) [2]
 - ☐ Uninitialized Memory Corruption Vulnerability
 - ☐ Microsoft Internet Explorer 6 is installed [4]
 - ☐ Microsoft Windows Server 2003 SP2 (x86) is
 - ☐ Microsoft Internet Explorer 7 is installed [2]
 - ☐ Microsoft Internet Explorer 8 is installed [2]

Uninitialized Memory Corruption Vulnerability

OR

Uninitialized Memory Corruption Vulnerability

AND

Mshtml.dll version is less than 6.0.2900.6049

Microsoft Windows XP (x86) SP3 is installed

Microsoft Internet Explorer 6 is installed

AND

Close



AGENDA

1	Information Security Challenges
2	Solutions
3	Types Of Controls
4	OVAL: A Closer Look
5	XCCDF
6	Conclusions



XCCDF Goals

- Document generation
- Expression of policy-aware configuration rules
- Support for conditionally applicable, complex, and compound rules
- Support for compliance report generation and scoring
- Support for customization and tailoring



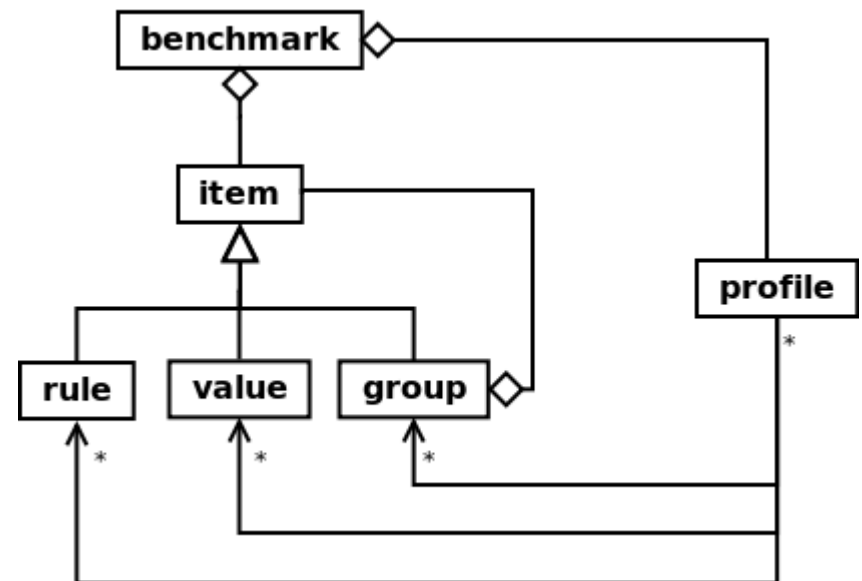
XCCDF Data Model

1. **Benchmark**

2. **Item**

named part of a benchmark

- **Group**
can hold other items
- **Rule**
holds check references
- **Value**
named data which can be tailored



3. **Profile**

references to Rule, Group, and Value Objects



XCCDF Rule

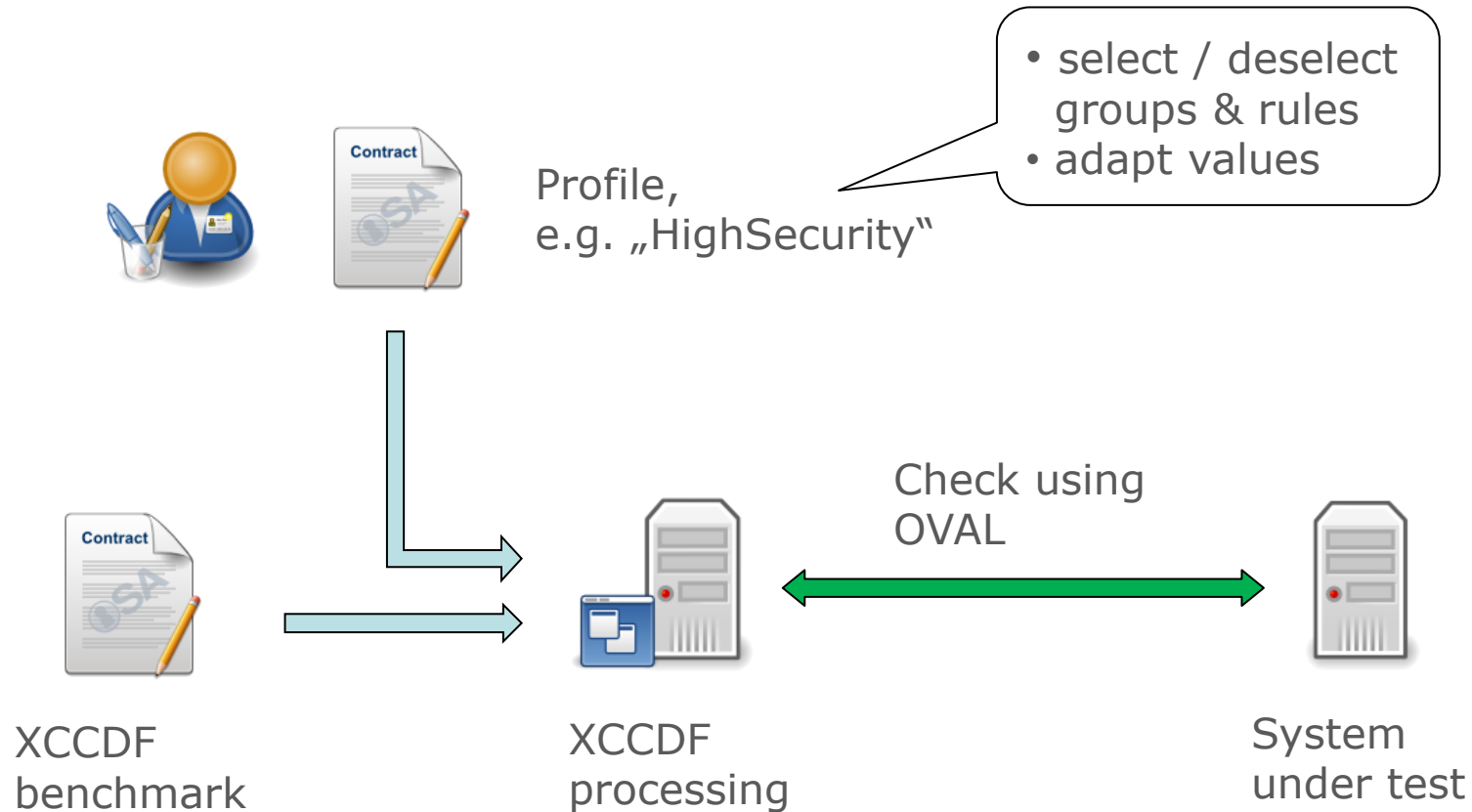
- XCCDF utilizes OVAL or OCIL
- CPE is used for identifying systems



```
<Rule id="cacls.exePermissions" selected="false" weight="10.0">
  <title>cacls.exe Permissions</title>
  <description>Failure to properly configure ACL file and directory permissions, allows the
    possibility of unauthorized and anonymous modification to the operating
    system and installed applications.</description>
  <reference>
    <dc:type>GPO</dc:type>
    <dc:source>Computer Configuration\Windows Settings\Security Settings\File System</dc:source>
  </reference>
  <requires idref="CM-6" />
  <requires idref="AC-3" />
  <ident system="http://cpe.mitre.org">CCE- 2726- 8</ident>
  <ident system="cpe.mitre.org/version/4">CCE- 977</ident>
  <check system="http://oval.mitre.org/XMLSchema/oval-definitions-5">
    <check-content-ref href="fdcc-winxp-oval.xml" name="oval:gov.nist.fdcc.xp:def:131" />
  </check>
</Rule>
```



Applying XCCDF Benchmarks





AGENDA

1	Information Security Challenges
2	Solutions
3	Types Of Controls
4	OVAL: A Closer Look
5	XCCDF
6	Conclusions



Advantages of Standards and Automation

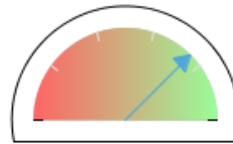
- Security content can be transferred easily
- Effort for checks is reduced drastically
- Expert knowledge is recorded as definitions
- Existing security guidance can be used easily
- Security checks are documented automatically
- Time for detection of security flaws is reduced
- Security becomes measurable
- Trends become visible



Results

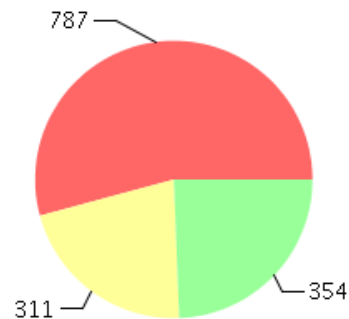
UPW Compliance Guard - Overview

Compliance Level

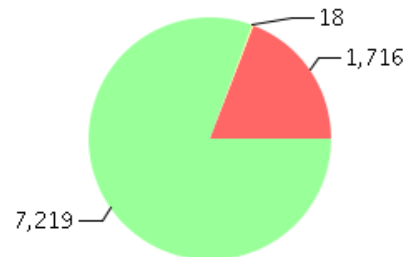


Compliance

- Bad
- Error
- Good
- Inventory exists
- Inventory not exists
- Other

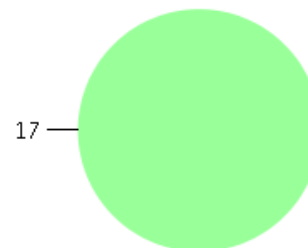


Vulnerability

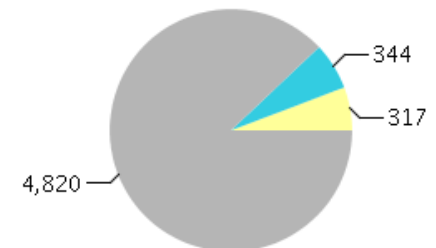


Miscellaneous

Patch



Inventory





Conclusions

- There are industry standards that make the automation of compliance requirements possible
- Automation of security checks increase the security level
 - More systems can be checked
 - Constant quality of checks
 - Checks can be repeated as often as you like
- High level of transparency:
Management, IT operations, auditor, compliance & security officer



Questions ?