



Ninth Software Assurance Forum

Andras R. Szakal

Chief SW Architect
IBM Distinguished Engineer
IBM Federal SW Group

Security and Compliance

Customer Compliance Challenges

Companies face increased pressure to achieve and maintain compliance – all with limited resources, time and budget.

- **AMR Research: North American Companies are estimated :**
 - ▶ To spend \$29.9B on regulatory compliance
 - ▶ \$8.8B on technology solutions
 - ▶ Technology solutions provide high degree of automation, more efficient, provide better IT Governance, Business and IT more efficient.

- **IBM Requirements Gathering Effort**
 - ▶ Cross Industry Collaboration
 - ▶ Financial, Entertainment, Telecom, etc
 - ▶ Collaboration with Compliance Insight
 - ▶ Consultants and Business Service Providers
 - ▶ Solutions Providers

- **Customers Looking for Compliance Automation Solutions**
 - ▶ Compliance Automation Solutions
 - ▶ Configuration in large scale enterprises
 - ▶ Heterogeneous device independent solution
 - ▶ Single solution for consolidating and automating multiple compliance regulations and standards.
 - ▶ Audit reporting to satisfy disparate compliance organizations.



- **43% of CFOs think that improving governance, controls and risk management is their top challenge.**

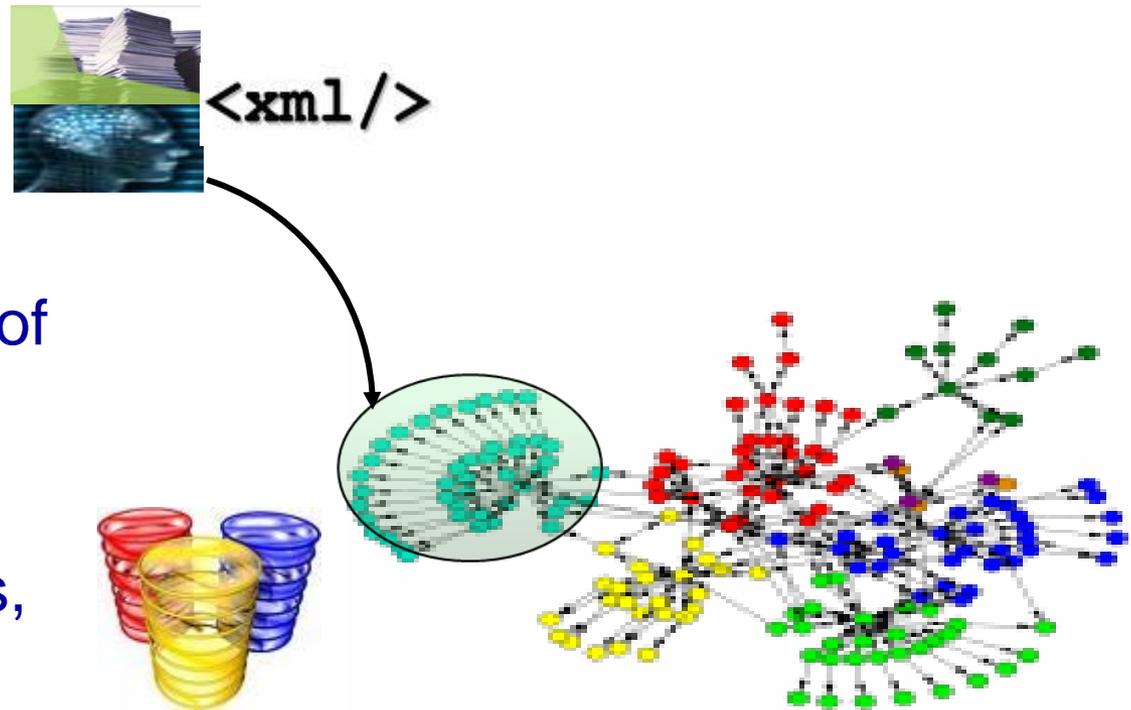
64% of CIOs feel that the most significant challenges facing IT organizations are security, compliance and data protection

CFO Survey: Current state & future direction, IBM Business Consulting Services

IBM Service Management Market Needs Study, March 2006

Overview of Common Industry Compliance Automation Tools

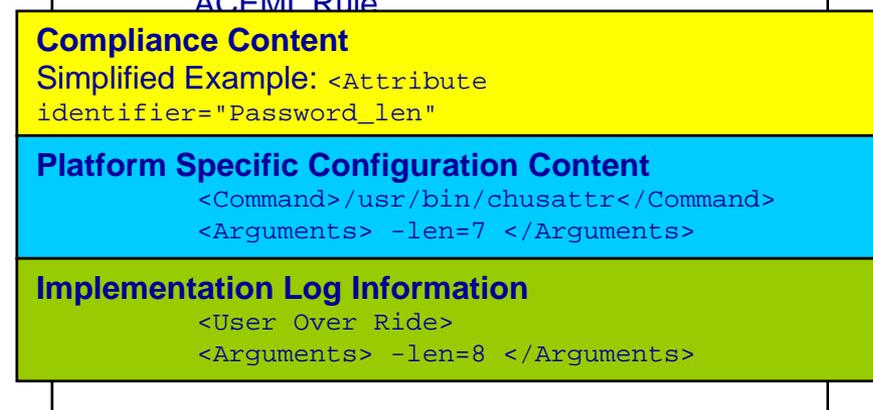
- Select Compliance Requirements
- Apply configuration policy to agnostic set of systems
- Monitoring for non-compliance alerts, audits reports
- Ease of Use, Manageable, Director Based, Scalable



Requirements for Compliance XML Standard

- Customer requirements drive the need for an XML standard.
- Standard must contain elements beyond standardized tags and content.
- Standard must facilitate all phases and methodology of compliancy.
- Standard must autonomously describe all phases: compliance requirement intent, mapping to device specific configuration action, configuration result, and monitor result.

Three Sections of Single ACEMI Rule



Life Cycle of Compliance Specification – View of Single Rule

1) Compliance Organization Mandates Rule



2) Compliance XML
Downloaded and Imported into to Automation Application (AA). AA maps Compliance Rule to device specific command.

3) Automation Application applies the configuration rule and documents the result back into the XML.

- Password Min Length
- 7
- “8.5.10 Require a minimum password length of at least seven characters”

Result of applied configuration rule



The benefit is that the final completed form of the rule autonomously describes:

- The intent of the compliance organization
- How this intent was mapped to a actionable command by the AA tool
- The result of applying the configuration command to the underlying device

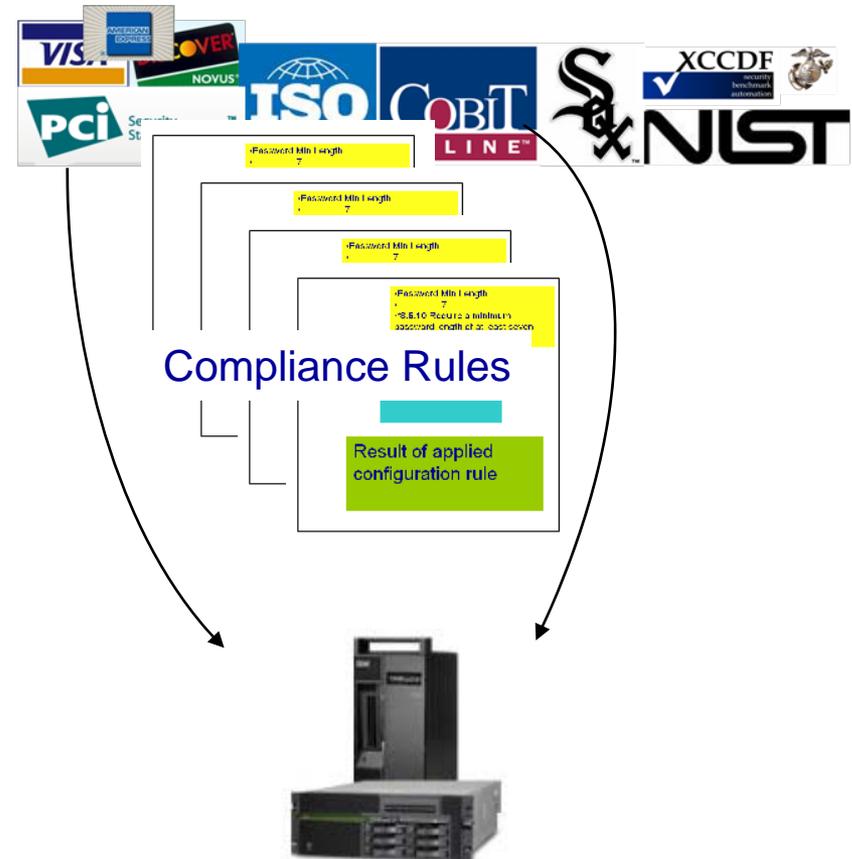
Single Systems - Multiple Compliance Requirements

Customer Pain Point

- Single systems must meet compliance requirements from multiple disparate regulations.
- Separate Audits from different compliance organizations

Customer Requirements

- Compliance Automation tools must be able to facilitate variances in compliance rules.
- Audit reports must be automated to reflect resolution of differing compliance specifications.
- Audit reports must reflect operator overrides and justifications



Reconcile Conflicting or Inconsistent Compliance Requirements Between Different Compliance Policies

- **Compliance Automation Tools must be able to reconcile similar rules which may conflict between to compliance standards.**
- **Apply a single configuration to the system that satisfies multiple compliance requirements.**

- Password Min Length
- 7
- “8.5.10 Require a minimum password length of at least seven characters. – PCI ”

Reconciliation Element

Elements for device specific mapping.

Elements to log device implementation results.

Reconcile Conflicting or Inconsistent Compliance Requirements



• Password Min Length
• **7**
• “8.5.10 Require a minimum password length of at least seven characters.”

• Password Min Length
• **8**
• “Internal Corporate Security Policy - Require a minimum password length of at least eight characters. – My corporation ”

• Password Min Length
• **8**
• “Security Policy - Require length of at least eight characters. – My corporation ”

Re

) “

Elements for device specific

/usr/sbin/chuser
passwd_len = 8

specific mapping.

Elements to log device implementation

Elements to log device implementation results.

implementation results.



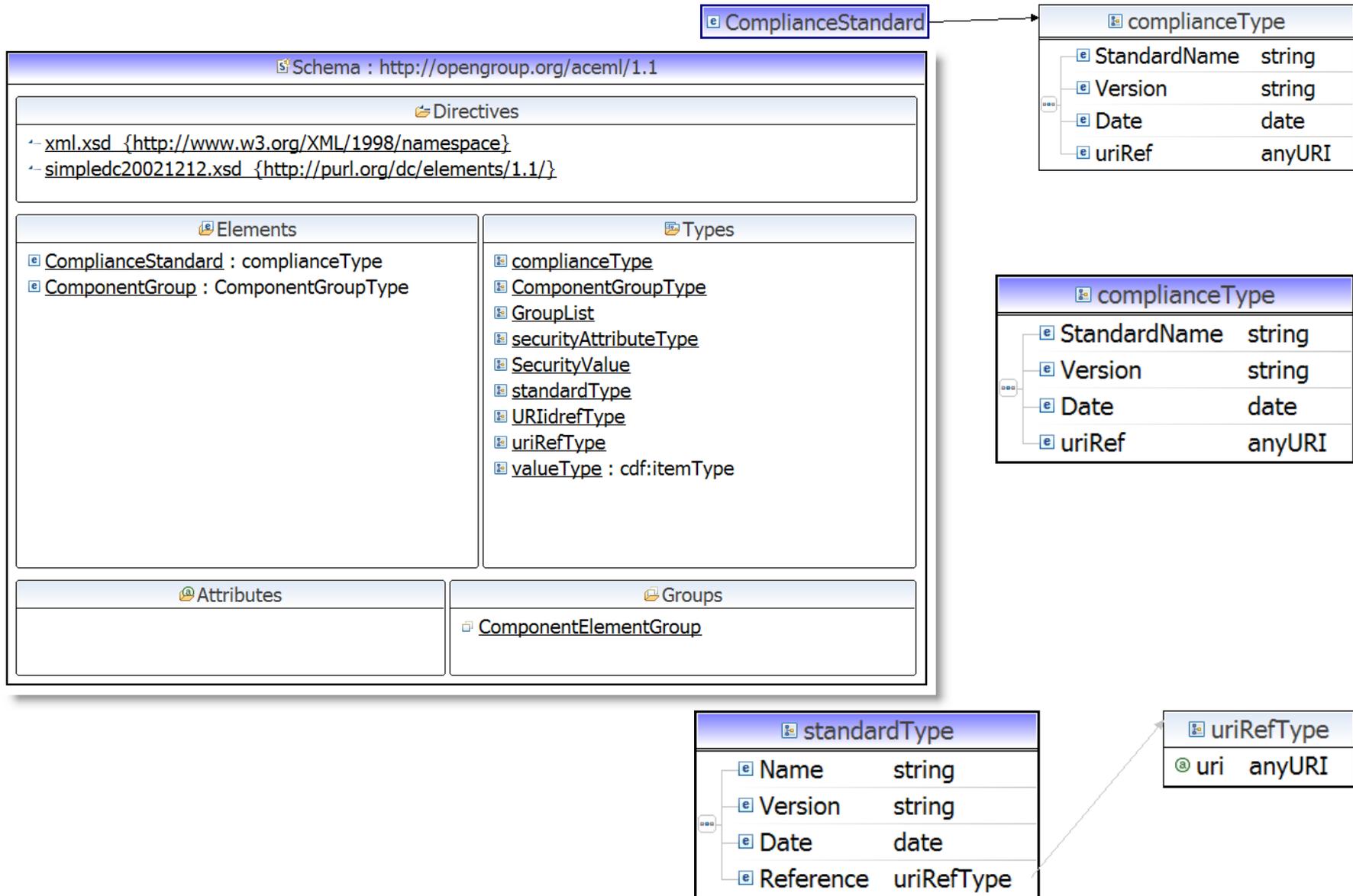
Compliance Automation Tool Reconciles Different Rule Specifications

Thanks!

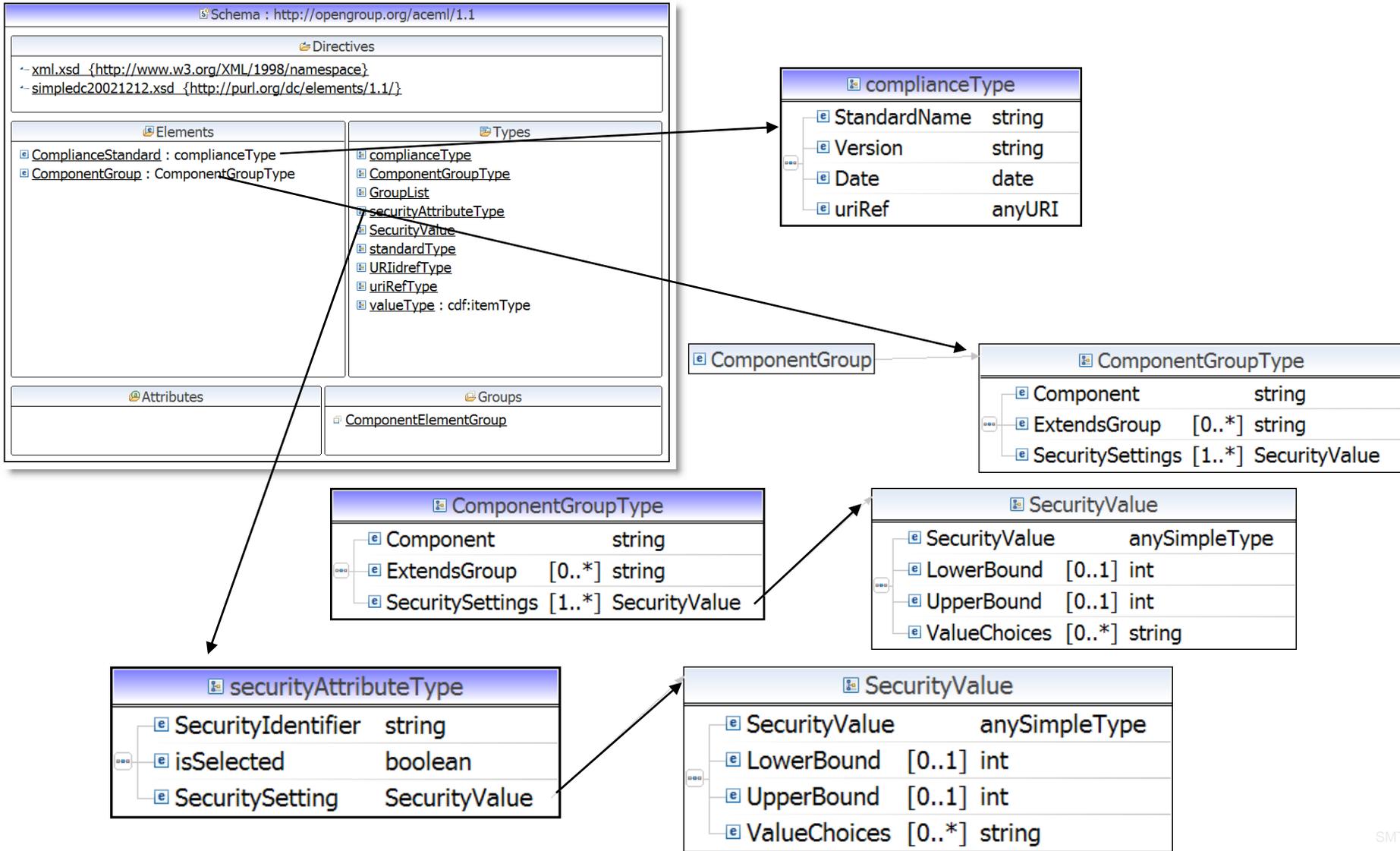
We invite you to join the discussion!

Backup Charts

ACEML 1.1



ACEML 1.1



ACEML 1.1

