



# Automated Compliance Expert Open Standard

**Shawn Mullen – IBM**  
AIX Security Architect  
[smullen@us.ibm.com](mailto:smullen@us.ibm.com)

The Open Group  
Automated Compliance Expert – Working Group

# Customer Compliance Challenges

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

**“The economic consideration of security can be more important than the technical considerations.” - Schneier**



## ■ 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**

## • 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*



# Security



## Customer Collaboration and Requirement Gathering

### 70 Companies

**CitiGroup**  
**FirstData**  
**US Gov (DoD)**  
**Lloyds**  
**ESPN**  
**Enterprise**  
**ILantus**  
**Technical Universites**  
**IBM Research**

## Customer Pain Points

- Cost of Compliance
  - Manual configuration
  - home-grown configuration scripts difficult to maintain and audit
- Companies and systems must meet multiple compliance regulations
  - PCI, SOX/COBIT, Internal Security Policies, US Gov.
- Compliance Audits:
  - Time consuming
  - Expensive
  - Auditors/Audits are not consistent

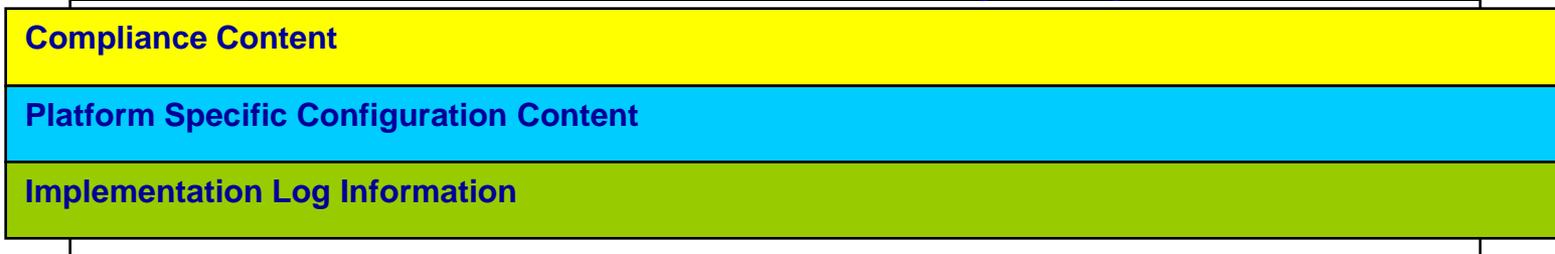
## Desired Features

- Automated Security and Compliance Configuration
- Automated Monitoring
- Standardized Compliance
- Combines Multiple Compliance Requirements
- Platform Independent
- Complete Audit Reporting
- Compliance Over Ride and Policy Authoring





### Three General Sections Security Compliance



# Virtualization / Cloud Computing

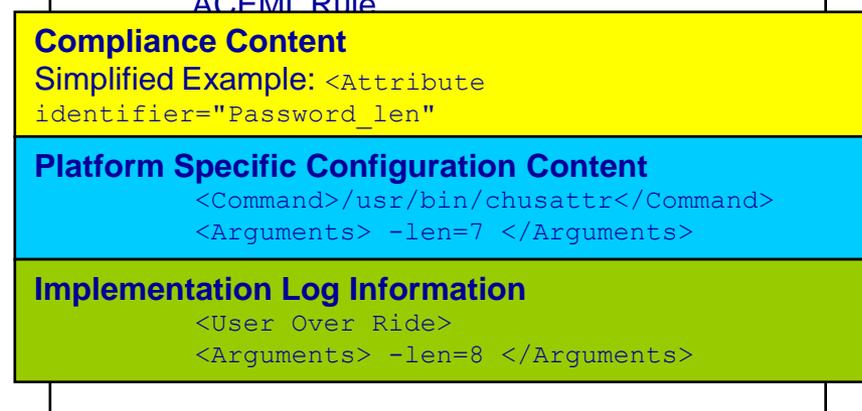
## Secure Virtual Machines



# 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  
ACEMt 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.

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

Result of applied configuration rule

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



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

# Overview of Common Industry Compliance Automation Tools

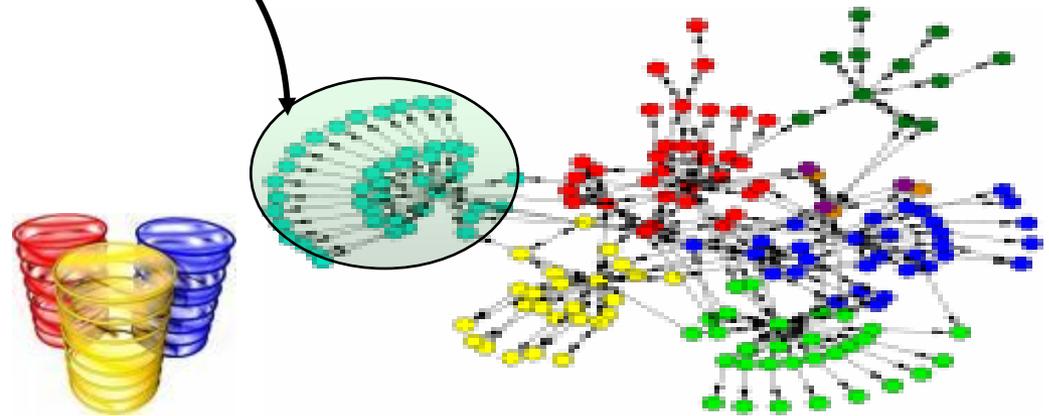
- Select Compliance Requirements



- Apply configuration policy to agnostic set of systems

- Monitoring for non-compliance alerts, audits reports

- Ease of Use, Manageable, Director Based, Scalable





# PCI-DSSv2 mapping to ACEML 1<sup>st</sup> draft 1/29/09

## Payment Card Industry Data Security Standard version 2 Automated Compliance Expert Rules

This worksheet reviews PCI-DSS requirements which might be possible to configure and check in an automated process.

<b>Column Discriptions:</b>	
<b>PCI-DSS Section</b>	This column provides a reference to the PCI requirement or section being addressed by this row of the worksheet.
<b>PCI Test Description</b>	This column describes how PCI recommends auditors test systems for meeting this requirement.
<b>Component</b>	PCI generalizes components as Server, Network or Application.
<b>ACEML Description</b>	This column provides a brief description or approach on the script that can be written to support and automate the PCI requirement.
<b>ACEML Label</b>	This is a ACEML label suggestion. "Report" lables will only report or monitor, but will not be able to set a configuration to meet a requirement.
<b>Value</b>	This column lists the value to set in ACEML and passed to the underlying script.
<b>Range</b>	This column lists the possible range of values which would still be acceptable in meeting the PCI requirement. This is the ACML reconciliation ra
<b>Device Specific</b>	This is not part of the PCI standard, but obviously some requirements apply only to specific types of devices, such as routers, or laptop and may

PCI-DSS Section	PCI Test Description	Component	ACEML Description	ACEML Label	Value	Range	Device Specific
<b>Build and Maintain a Secure Network</b>							
	Verify that there is a formal process for testing and approval of all network connections and changes to		Turns on Audit log of any configuration changes to network settings.				
	1.1.1 firewall and router configurations.	Network		Audit_Network_Config	On	On	None Specific
	1.1.5 Verify that firewall and router configuration standards include a documented list of services, protocols and ports necessary for business—for example, hypertext transfer protocol (HTTP) and Secure Sockets Layer (SSL), Secure Shell (SSH), and Virtual Private Network (VPN) protocols.		Reports all open network ports and describes which ports are secure/encrypted and which are open / clear text				
	1.1.5.a Identify insecure services, protocols, and ports allowed; and verify they are necessary and that security features are documented and implemented by examining firewall and router configuration standards and settings for each service. An example of an insecure service, protocol, or port is FTP, which passes user credentials in clear-text.	Network		Report_Open_Network_Ports	N/A	N/A	None Specific
	1.1.5.b 1.2.1.a Verify that inbound and outbound traffic is limited to that which is necessary for the cardholder data environment, and that the restrictions are documented.	Network	Turns off well known clear text password and weak authentication ports, i.e. telnet, ftp, rlogin, rcp, etc.	Network_Prohibit_Clr_Text_Passwds	On	On	None Specific
	1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.	Network	Allows inbound/outbound traffic for only a range or set of ports, and denies all other port traffic.	Network_Allowed_Ports	range or set	range or set	None Specific

## ACE-WG Moving forward

- **Continue collaboration with:**
  - NIST
  - Payment Card Industry
  - DoD
  - others
- **Common Criteria new Operating System Protection Profile (OSPP)**
- **Planned to Finalize Standard later this year.**



