The Open Group

February 3 – 6th, 2009 – San Diego

THE Open GROUP
Making standards work®

Automated Compliance Expert Working Group

Shawn Mullen

AIX Security Architect

smullen@us.ibm.com

PowerVM

Agenda

- **Economics of Security and Compliance**
- **Security and Compliance**
- **Automated Compliance Expert**
  - **Working Group**
  - **Standard**

Compliance Driven By Economics

- Security Failures = Economic Failures
- No more viruses…
  - … that kill the host
- Gone are the innocent days of web site defacing.
  - Cybercriminals fast-flux hide their content servers
  - Storm Network leased out
  - 10 million PCs, supercomputer power
  - Spam, phishing, illicit websites

IBM BlueGene/L Super Computer

Security, Cryptography, Compliance History

- Marketing divided in to Fear or Greed
- Fear is a difficult sell
- Cost of Damage x %risk = amount to spend on Security
- Cost of Damage is infinity and risk is 0
- 0 x infinity = non-determinant
- Mary Queen of Scotts
- Queen Elizabeth I
- Sir Francis Walsingham
- Letters to Anthony Babington
- al-Kindi House of Wisdom

Compliance changes Security to Greed Sale

- Compliance to Protect the Industry

  Payment Card Industry, Stock Market

- ATMs US vs. UK

- Litigation
- Penalties
- Compliance Regulations

  Card holder only responsible for $50 of loss.

- T.J Maxx / Marshalls 45.7 million credit cards stolen over 18 months
- Enron

ACE – WG

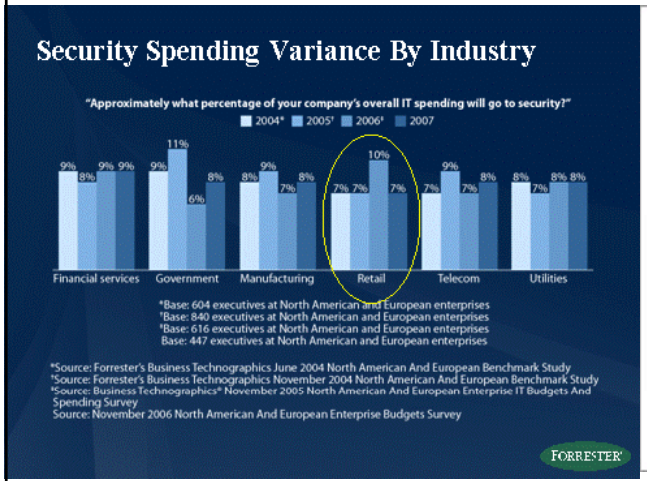
- HIPPA, PCI, SOX/COBIT, ISO, JSOX, etc
  - Peel the onion and find IT security in these standards
- Implement Compliance on Systems such that its benefits of uptime, IT Governance, and risk reduction outweigh costs.
- AMR $8.8B spent on compliance technology solutions

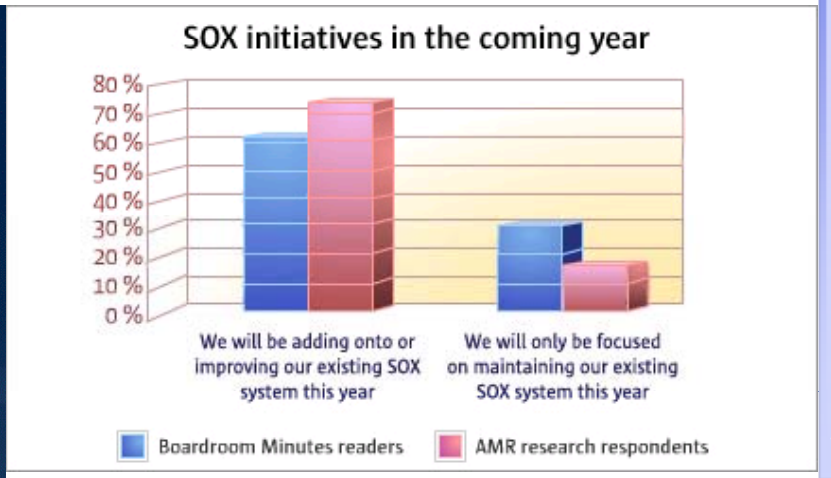
- **43% of CFOs think that improving governance, controls and risk management is their top challenge.**

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

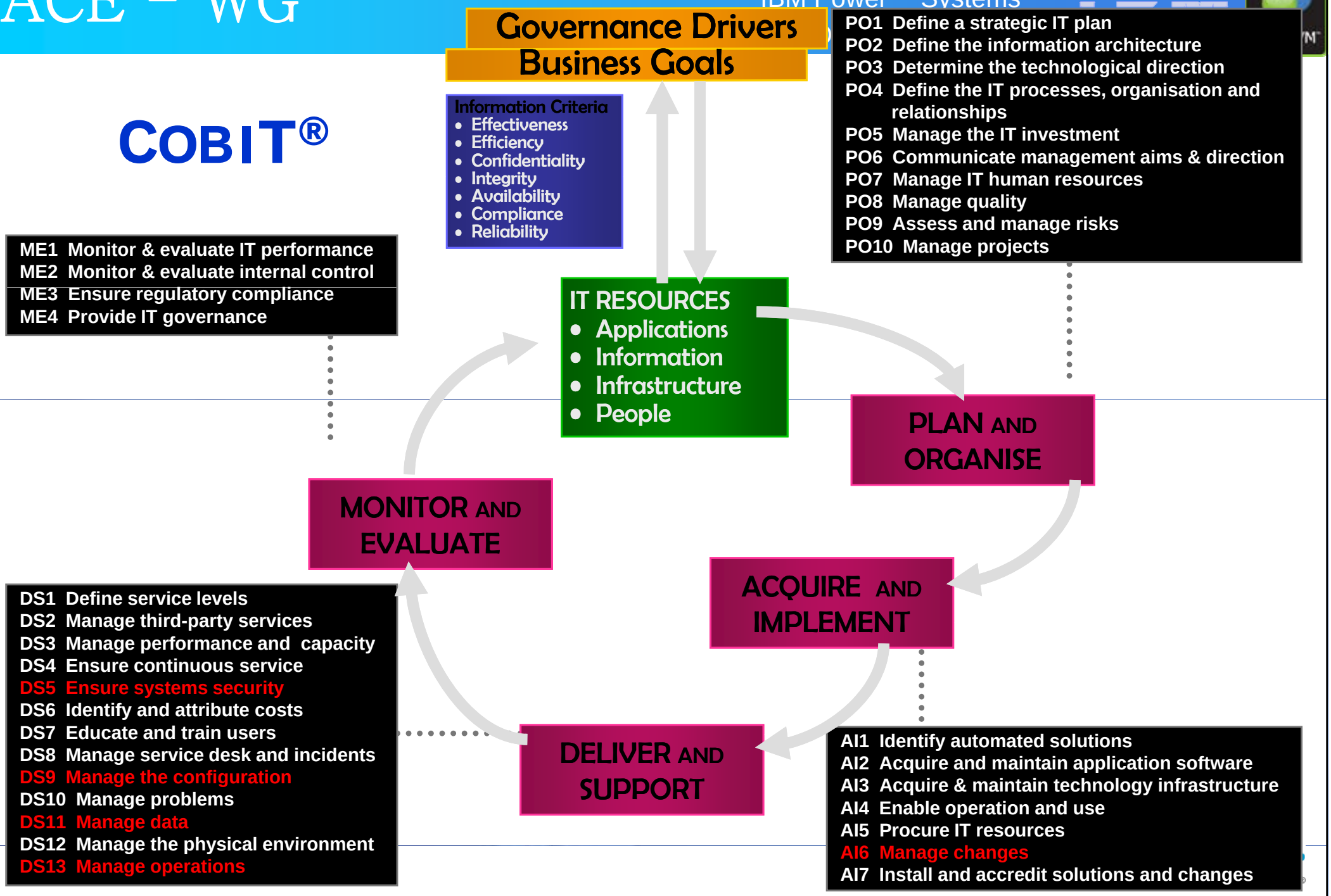
CFO Survey: Current state & future direction, IBM Business Consulting Services

IBM Service Management Market Needs Study, March 2006



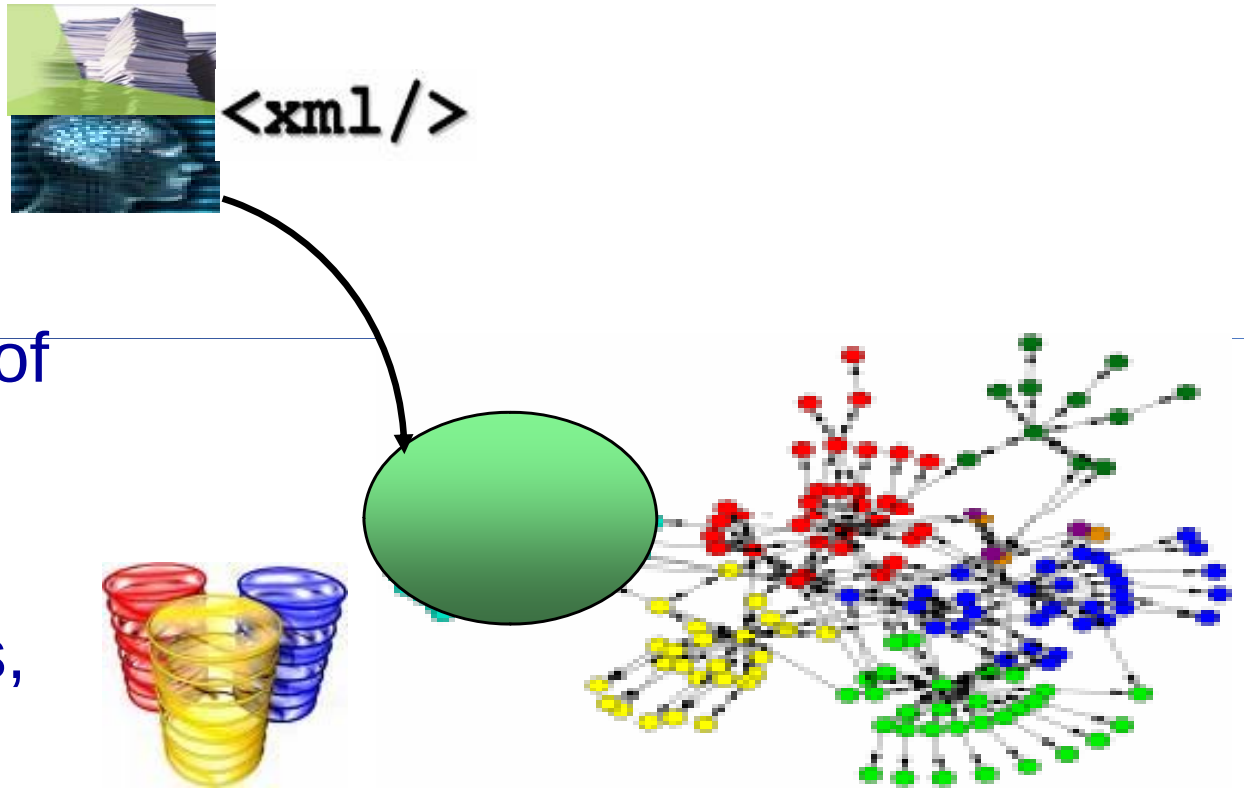


COBIT®


Governance Drivers
Business Goals
Information Criteria
• Effectiveness
• Efficiency
• Confidentiality
• Integrity
• Availability
• Compliance
• Reliability
PO1 Define a strategic IT plan
PO2 Define the information architecture
PO3 Determine the technological direction
PO4 Define the IT processes, organisation and relationships
PO5 Manage the IT investment
PO6 Communicate management aims & direction
PO7 Manage IT human resources
PO8 Manage quality
PO9 Assess and manage risks
PO10 Manage projects
ME1 Monitor & evaluate IT performance
ME2 Monitor & evaluate internal control
ME3 Ensure regulatory compliance
ME4 Provide IT governance
IT RESOURCES
• Applications
• Information
• Infrastructure
• People
PLAN AND ORGANISE
ACQUIRE AND IMPLEMENT
DELIVER AND SUPPORT
MONITOR AND EVALUATE
DS1 Define service levels
DS2 Manage third-party services
DS3 Manage performance and capacity
DS4 Ensure continuous service
DS5 Ensure systems security
DS6 Identify and attribute costs
DS7 Educate and train users
DS8 Manage service desk and incidents
DS9 Manage the configuration
DS10 Manage problems
DS11 Manage data
DS12 Manage the physical environment
DS13 Manage operations
AI1 Identify automated solutions
AI2 Acquire and maintain application software
AI3 Acquire & maintain technology infrastructure
AI4 Enable operation and use
AI5 Procure IT resources
AI6 Manage changes
AI7 Install and accredit solutions and changes

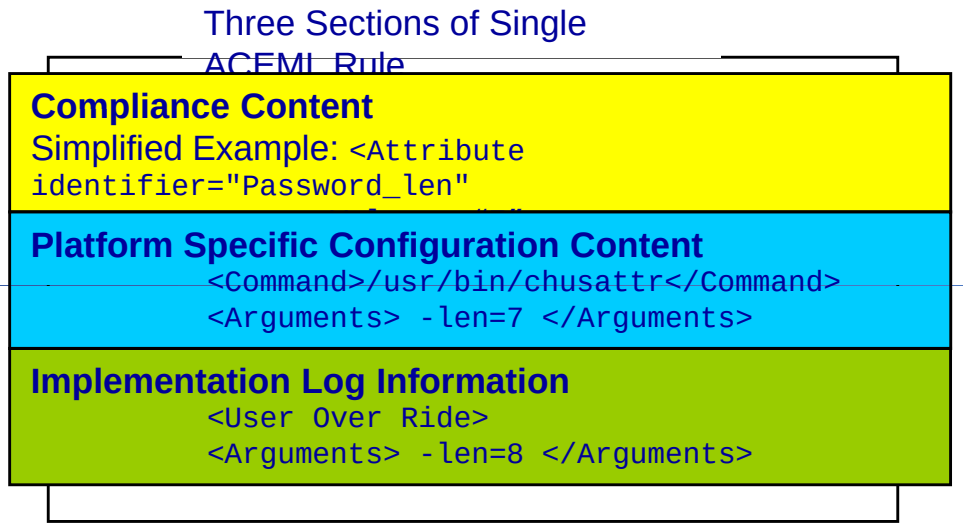
Automated Compliance Expert Automation Tools

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



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.



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 c

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

ACE – WG

IBM Power™ Systems
The Open Group

Reference Target Audience

- This quick reference guide is intended for **anyone looking for a high level view of The Open Group's Automated Compliance Expert Compliance Standard.**
- Anyone looking for links to provide more detail.
- Anyone looking for a list of participants and a brief history of the ACE-WG work.

Value Proposition of this Standard

The Automated Compliance Expert (ACE) standard is being pursued by The Open Group as a method to automate security compliance configuration across multiple platforms and Operating Systems.
The ACE-WG solution will facilitate a standard xml and content around security and configuration. This standard will enable the development of technology and applications which can:

- Automatically configure devices based on compliance standards such as PCI, or COBIT.
- Allow compliance organizations to describe specific security configuration rules in a simple general form, independent of any underlying computer system
- Enable monitoring applications to precisely identify compliance and security configuration events and violations.
- Generate precise configuration and security audit reports.

Overview

- According to AMR Research, North American Companies are estimated to spend $29.9B on regulatory compliance and will spend $8.8B this year on technology solutions to solve their compliance requirements. Compliance costs worldwide are large and growing, and the need to comply is not an option. Reducing this cost is therefore a business imperative.
- The key components needed to reduce the cost of compliance are automation and a consistent reproducible process. The Automated Compliance Expert Working Group (ACE-WG) will create a knowledgebase format which can be consumed by compliance tools. These tools will be able to achieve a high degree of automated compliance configuration and monitoring. This in turn will reduce the cost of compliance for end users and increase security consistency amongst all of a company's IT systems.
- There are many different compliance standards. There are many areas of compliance within these standards. Not all elements of compliance can be automated. However, many of the compliance standards have overlapping guidance in the area of IT security and configuration. The Open Group can lead the way in providing an XML based compliance knowledgebase from which compliance automation tools can be built.

ACE Key Enabling Features

- Regulatory Compliance organizations can describe their required security and configuration rules in a high level manner, independent of OS or platform specifics.
- Corporations will be able to describe their own security configuration policies with this same high level XML and content.
- The ACE XML contains a straight forward method to reconcile differences between disparate policies when they are applied to a single system. Therefore, it is possible to apply PCI, SOX/COBIT, and internal security configuration policies onto a single system, in a automated manner, and still have the system meet all three compliance standards.
- Compliance monitoring is automated and greatly simplified. There is no need to log scrape to detect compliance violations.
- When a compliance violation does occur, the monitoring tool can provide a detailed description of the (mis)configuration parameter and a description of the compliance regulation and rule being violated.

The Open Group Participants

- Ian Dobson, Director of Security Forum
- Jim Hietala, Vice President of Security

Working Group Founders

- Capgemini
- CA
- IBM
- Qualys
- The Open Group

IBM Participants

- Shawn Mullen (ACE-WG Chair)
- Andras Szakal
- Guha Prasad Venkataraman
- Sandy Amin

Key Collaborators

- ***US Government***
  - NIST, in particular XCCDF, SCAP, and OVAL standards
  - NSA
  - DHS
- ***Open Compliance and Ethics Group***
- ***Payment Card Industry***
  - Proposed Relationship
- ***Cobit*** .
  - Proposed Relationship
- ***ISO Security***
  - Proposed Relationship
- ***Oasis***
  - Possible Relationship

Is ACE is not competing as another compliance standard.

ACE is not another regulatory compliance standard competing with the work in NIST/NSA/DHS, COBIT, ISO, PCI, OASIS, and elsewhere. Rather - the ACE standard will provide the means to describe in XML form the applicable regulatory compliance rules in a manner that is platform and OS independent.

- ACE is a XML schema and content which will facilitate the automated configuration of standards such as PCI, and COBIT.
- ACE will allow Compliance Organizations such as PCI, and COBIT to describe their required security configuration rules in standardized XML and content. This will allow end users to automate the configuration and monitoring of computer systems, regardless of the computer's operating system.
- It is the intent of the ACE-WG to work with Compliance Organizations, so they can publish their security configuration rules using ACE XML.

.

ACE-WG Public Documents

- The Open Group **ACE-WG Charter**
- Additional ACE-WG output is published on the ACE Website

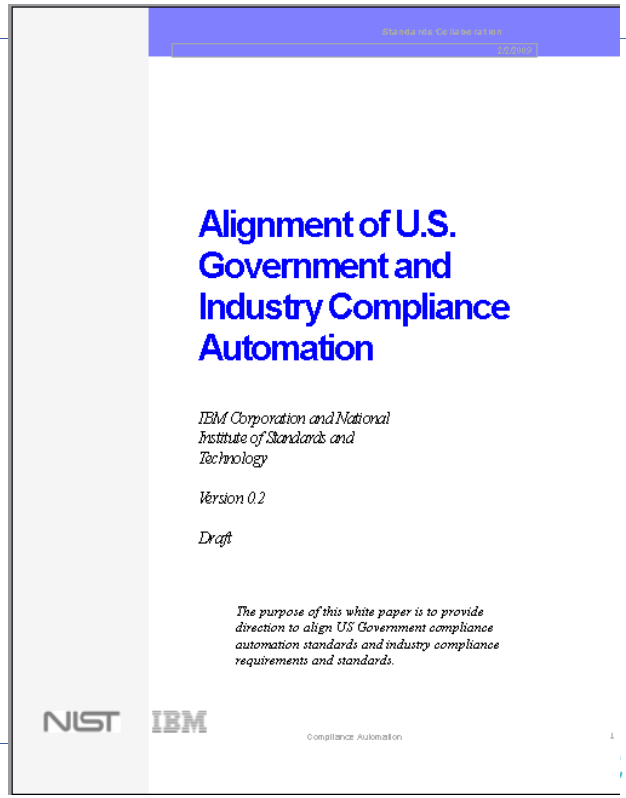
Summary

The ACE standard will allow any compliance organizations to publish their requirements using standardized XML and content. End users will be able to configure systems to adhere to one or multiple compliance organizations requirements.

This standard will greatly reduce system configuration time and simplify the audit process.

Magnified across large organizations with in multi-vendor IT environments, required to meet multiple regulatory compliances, ACE will be able to greatly reduce the cost and complexity of meeting regulatory compliance mandates.

- ACE-WG Overview on TOG security website
  - Benefits, Goals, Participants
  - Key Collaborators, NIST (SCAP), PCI
  - Customer Involvement



Open GROUP
Making standards work®

PCI-DSSv2 mapping to ACEML 1st 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.

Column Discriptions:	
PCI-DSS Section	This column provides a reference to the PCI requirement or section being addressed by this row of the worksheet.
PCI Test Description	This column describes how PCI recommends auditors test systems for meeting this requirement.
Component	PCI generalizes components as Server, Network or Application.
ACEML Description	This column provides a brief description or approach on the script that can be written to support and automate the PCI requirement.
ACEML Label	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.
Value	This column lists the value to set in ACEML and passed to the underlying script.
Range	This column lists the possible range of values which would still be acceptable in meeting the PCI requrirment. This is the ACML reconciliation ra
Device Specific	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	Componer	ACEML Description	ACEML Label	Value	Range	Device Specific
Build and Maintain a Secure Network							
1.1.1	Verify that there is a formal process for testing and approval of all network connections and changes to firewall and router configurations.	Network	Turns on Audit log of any configuration changes to network settings.	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.	Network	Reports all open network ports and describes which ports are secure/encrypted and which are open / clear text	Report_Open_Network_Ports	N/A	N/A	None Specific
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	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.	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. 1.2.1.b Verify that all other inbound and outbound traffic is specifically denied, for example by using an explicit “deny all” or an implicit deny after allow statement.	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