THE Open GROUP
Making standards work®

Automated Compliance Expert Open Standard

Shawn Mullen - IBM

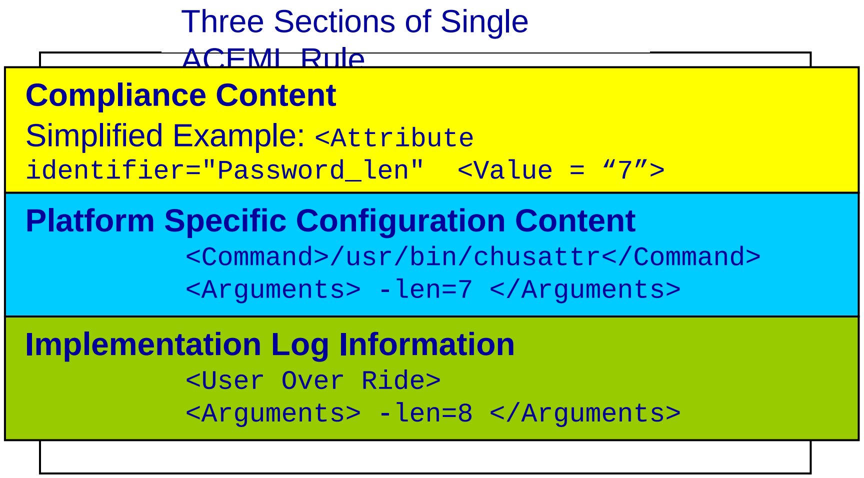
Requirements for Compliance XML Standard

- 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 ACEML Rule

Compliance Content

Simplified Example: `<Attribute identifier="Password_len"  <Value = “7”>`

Platform Specific Configuration Content

```
<Command>/usr/bin/chusattr</Command>
<Arguments> -len=7 </Arguments>
```

Implementation Log Information

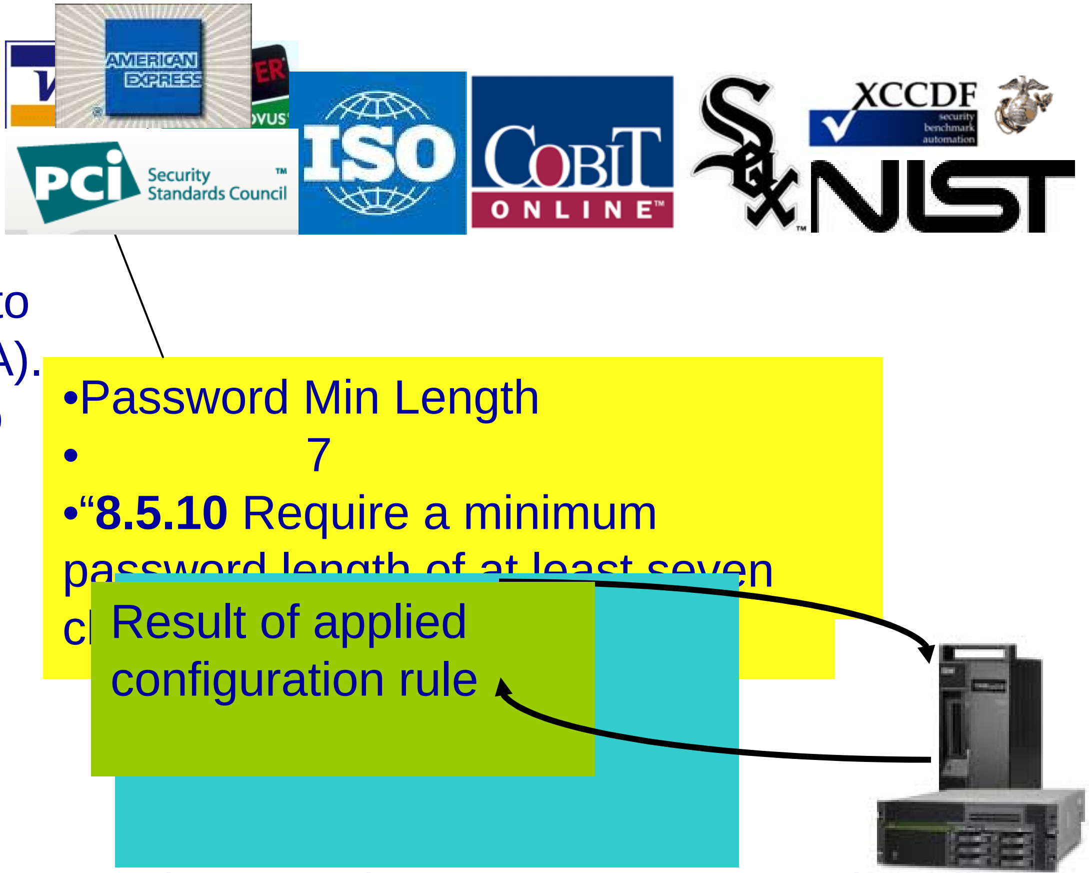
```
<User Over Ride>
<Arguments> -len=8 </Arguments>
```

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.


AMERICAN EXPRESS
PCI Security Standards Council
ISO
COBIT ONLINE
XCCDF security benchmark automation
NIST

•Password Min Length

• 7

•“**8.5.10** Require a minimum password length of at least seven cl

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

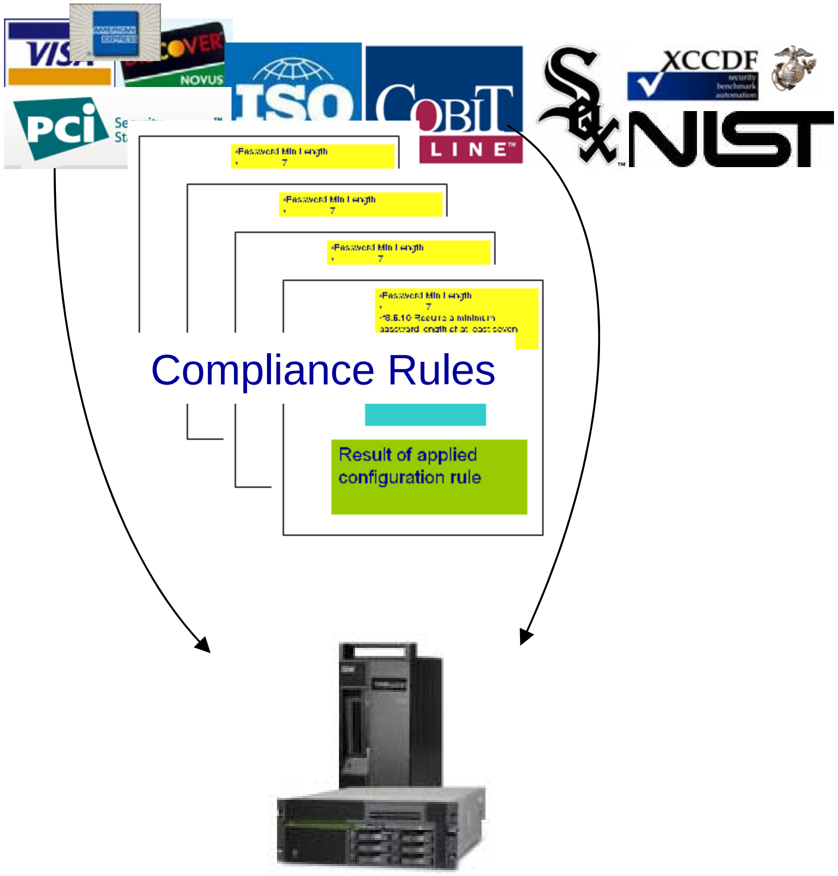
Single Systems - Multiple Compliance Requirements

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



SMT

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.

SMT

Reconcile Conflicting or Inconsistent Compliance Requirements

PCI Security Standards Council™

FOOFOO online.com

- Password Min Length
- 7
- “**8.5.10** Require a minimu at least seven characters.

Re

Elements for device specif

Elements to log device im

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

/usr/sbin/chuser passwd_len = 8

Elements to log device implementation results.

ı

Security Policy - Require length of at least eight ɔration ”

) “

ɔecific mapping.

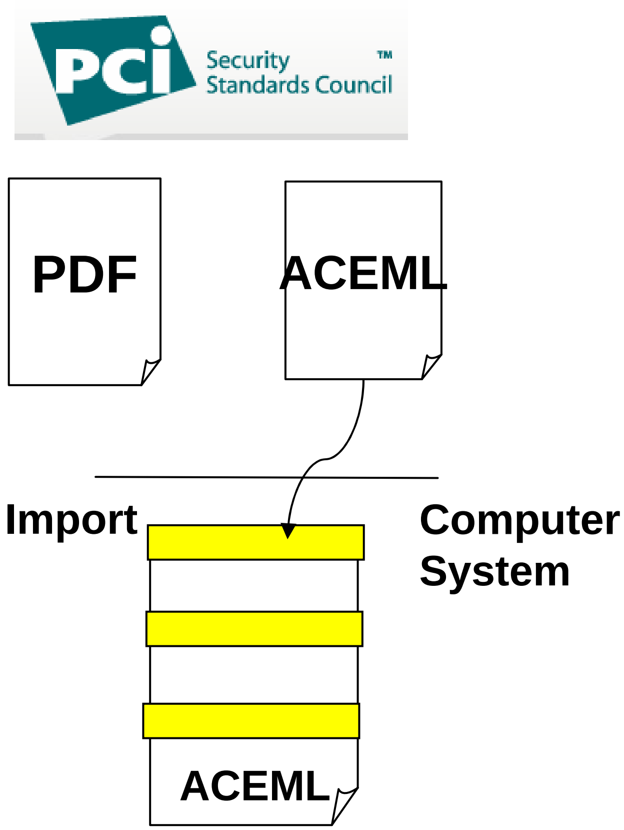
e implementation results.

Compliance Automation Tool
Reconciles Different Rule Specifications

SMT

ACEML General Process Flow

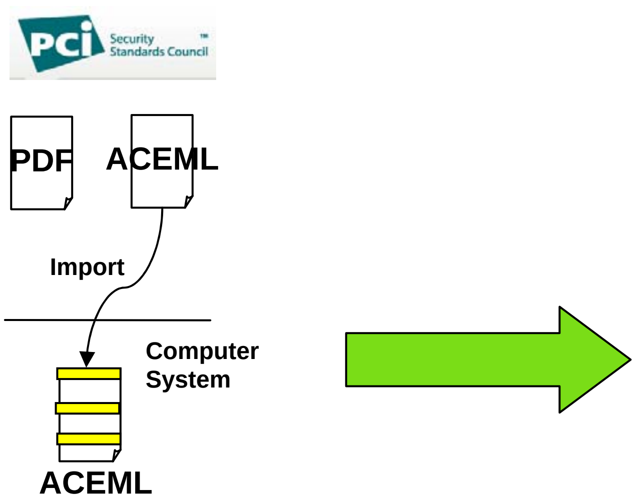
Compliance Organization
Publishes Requirements



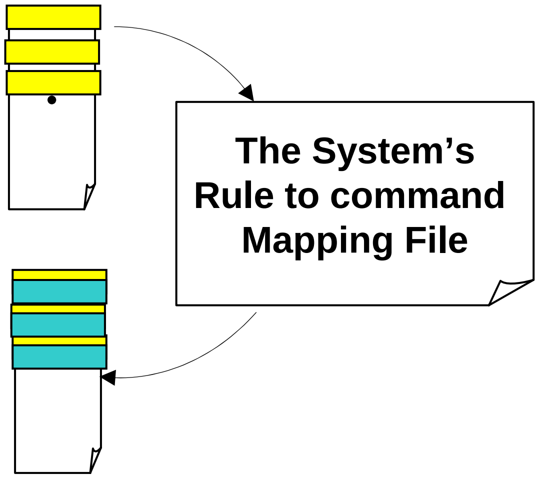
ACEML General Process Flow

Compliance Organization

Publishes Requirements



Mapping high level rules to actionable commands on the system end points



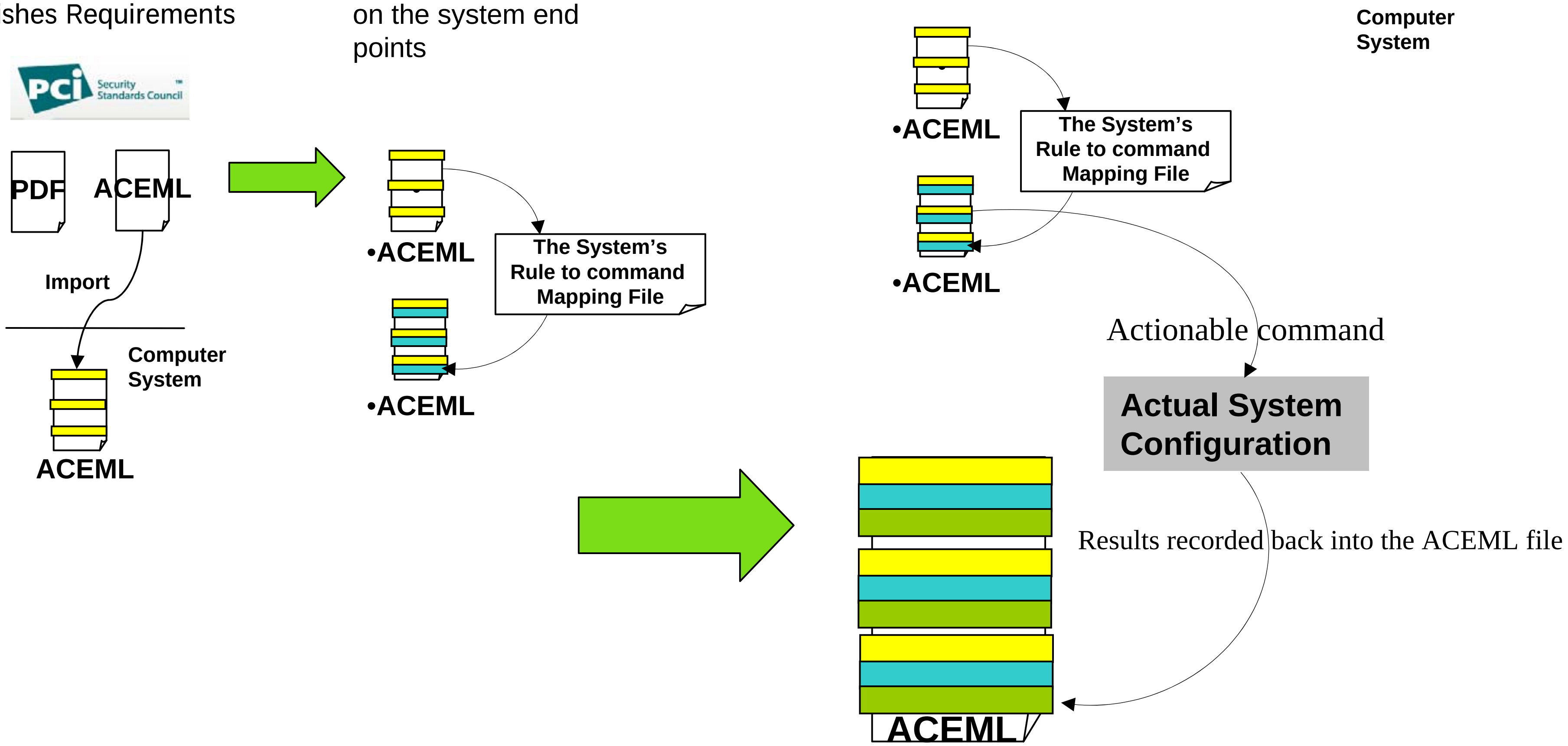
ACEML General Process Flow

Compliance Organization

Publishes Requirements

Mapping high level rules to actionable commands on the system end points

Apply Settings or Check Settings Complete audit and reporting artifacts



PCI Security Standards Council

PDF

ACEML

Import

Computer System

ACEML

•ACEML

The System's Rule to command Mapping File

•ACEML

Computer System

•ACEML

The System's Rule to command Mapping File

•ACEML

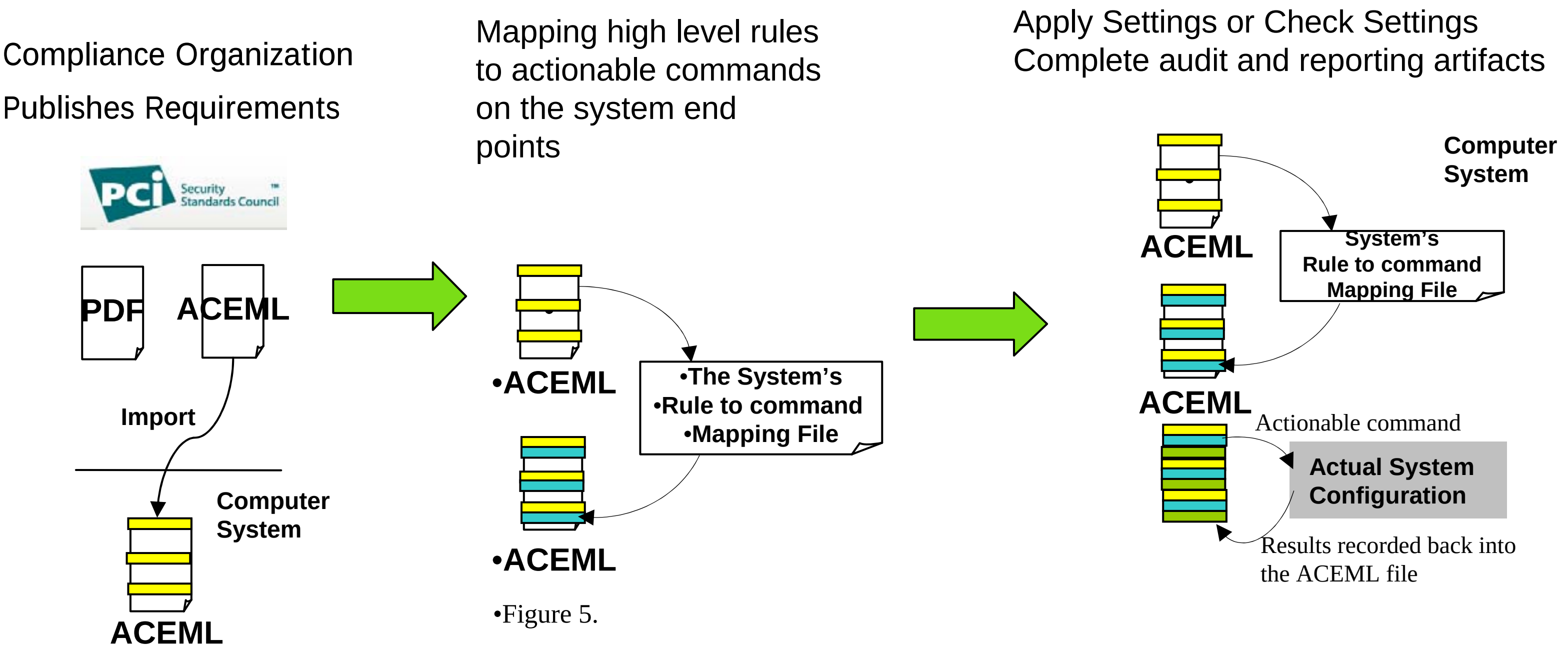
Actionable command

Actual System Configuration

Results recorded back into the ACEML file

ACEML

ACEML General Process Flow



Compliance Organization

Publishes Requirements

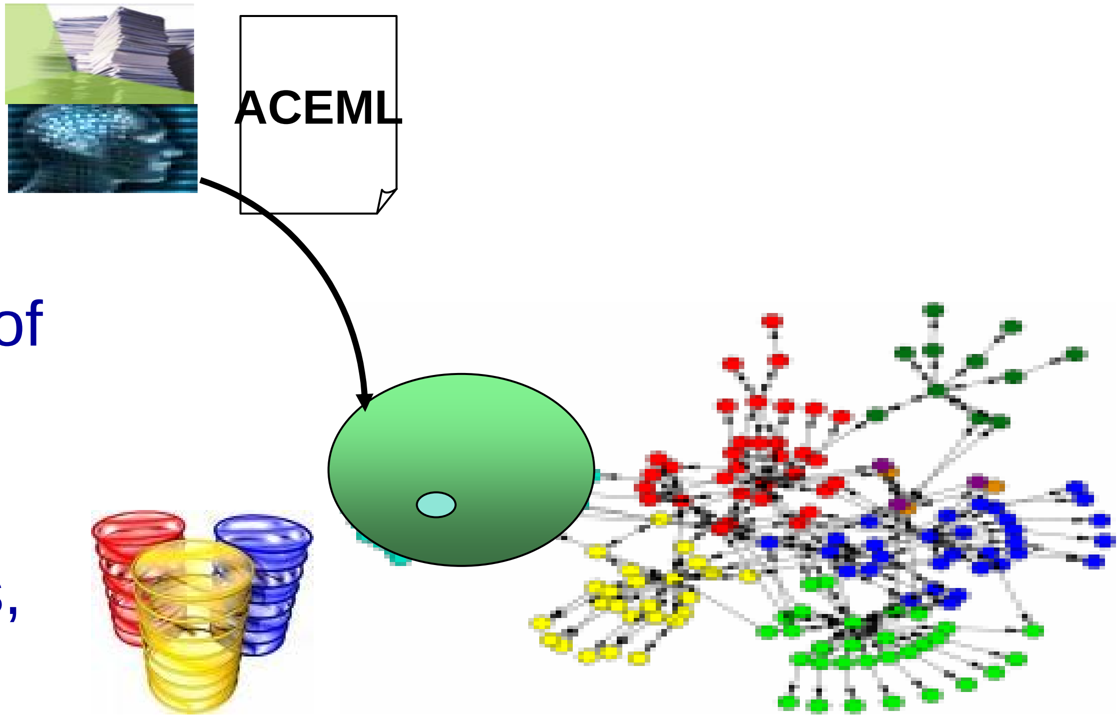
Mapping high level rules to actionable commands on the system end points

Apply Settings or Check Settings
Complete audit and reporting artifacts

•Figure 5.

Overview of Common Industry Compliance Automation Tools

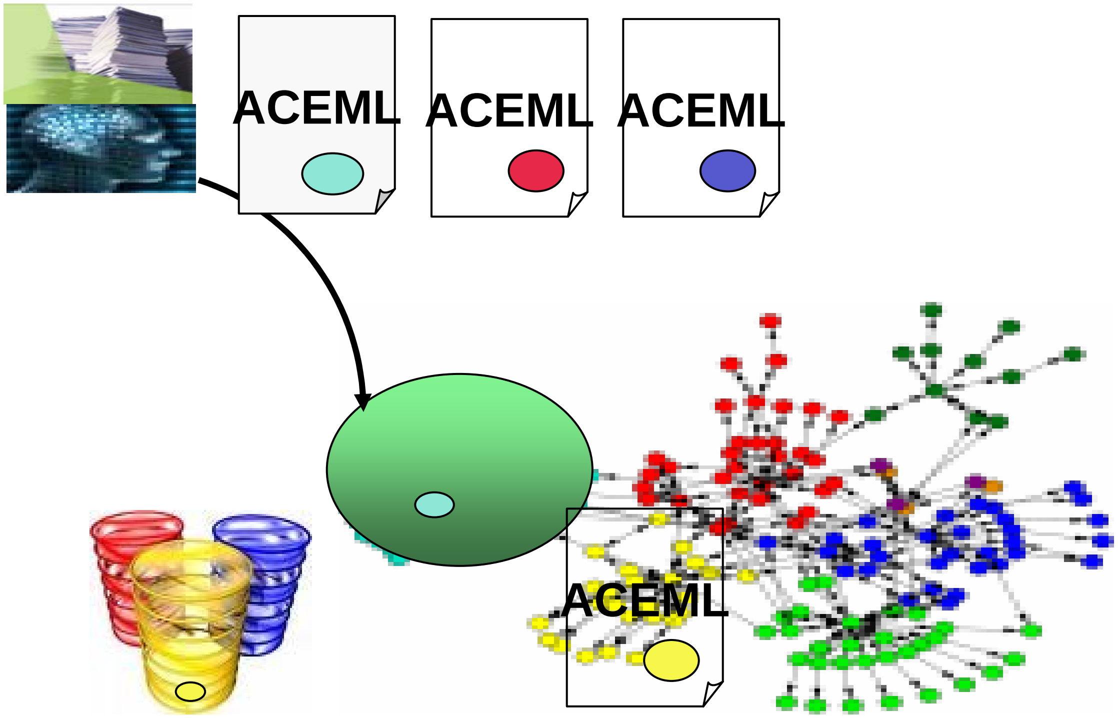
- Select Compliance Requirements
- Apply configuration policy to agnostic set of systems
- Monitoring for non-compliance alerts, audits reports
- Ease of Use, Manageable, Director Based, Scaleable



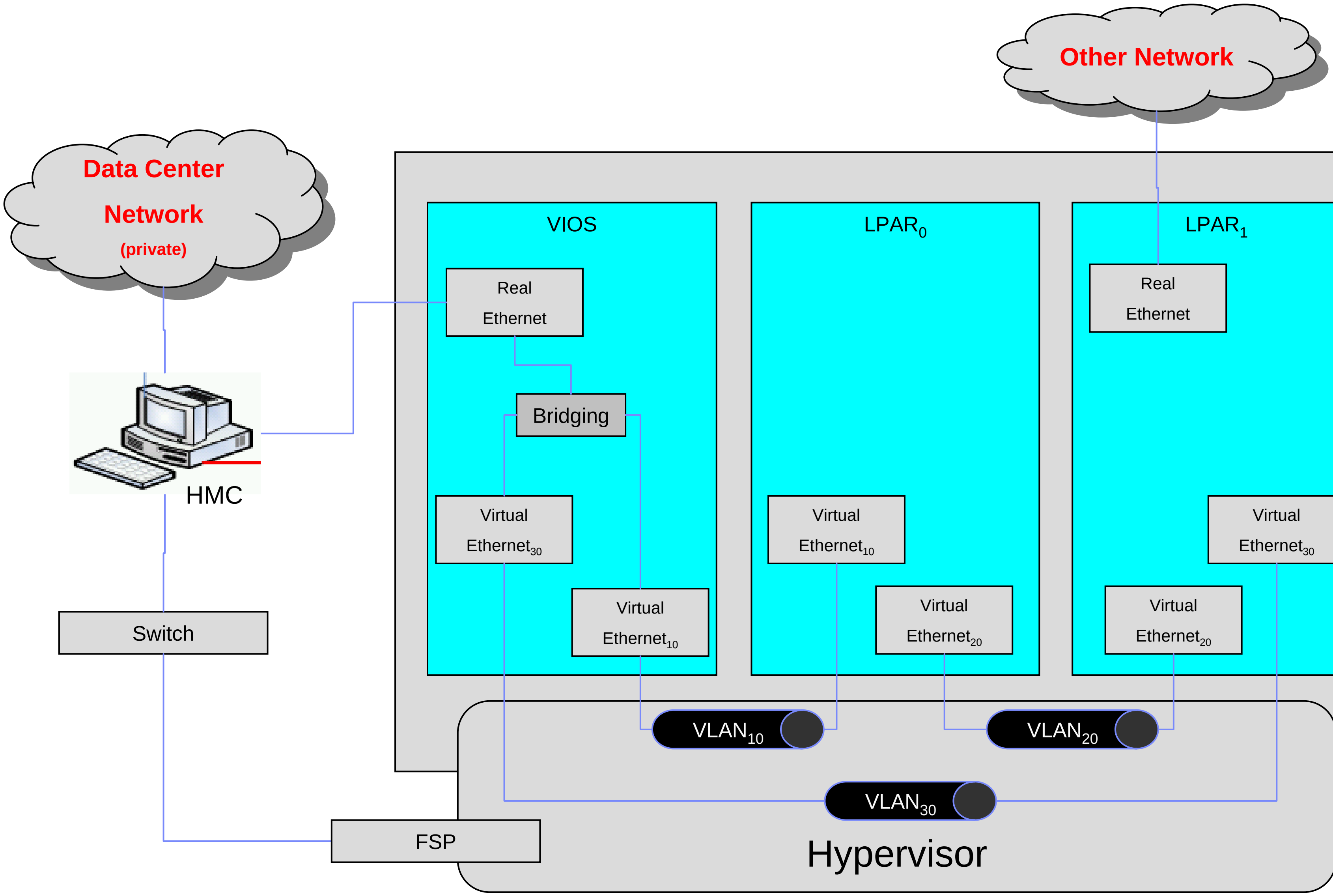
SMT

Security and Compliance within the Cloud Environment

- Virtualized / Cloud Environments
- ACEML is Compliance Focused
- Security Policy, Meta Data for Virtual Systems
- Build upon Authoring and Remediation abilities built into ACEML
- Cloud Mgt and Control Points: Secure Virtual Machine, Virtual System Configuration Console, VLAN, Virtual I/O System, Single Root – I/O Vector (SR-IOV) adapters.
- Exclusive management authorization on shared management infrastructure.



Basic System Architecture


Other Network
Data Center
Network
(private)
VIOS
$LPAR_0$
$LPAR_1$
Real
Ethernet
Real
Ethernet
Bridging
HMC
Virtual
$Ethernet_{30}$
Virtual
$Ethernet_{10}$
Virtual
$Ethernet_{10}$
Virtual
$Ethernet_{20}$
Virtual
$Ethernet_{30}$
Virtual
$Ethernet_{20}$
Switch
$VLAN_{10}$
$VLAN_{20}$
$VLAN_{30}$
FSP
Hypervisor