6th Annual IT Security Automation Conference and Expo
September 27-29, 2010, Baltimore Convention Center

Security Automation for the Cloud

Dennis R. Moreau, Ph.D.
Senior Technology Strategist
RSA Security

RSA
The Security Division of EMC

Cloud Computing Security: What's more difficult?

- Deeper technology stack
- More intimate sharing of resources
- More dynamic hosting
- Multi-Tenancy (Multi-department (-cy?))
- Composition of services; xCloud
- Composition of partners, supply chain, … trust network
- Homogeneity – cartography, advanced threats, …

Cloud Computing Security: The threat

- Advanced threats targeting cloud infrastructure and endpoints
- Discovery/mapping of workload to host binding for malware co-location
- Side channels through shared resources
- Isolation threats - firmware, glue chips, BIOS, …
- Authentication - blended roles, federation
- Information security - protection, availability, privacy

Cloud Computing Security: What can work better?

- Community sourced insight – content to efficacy
- Provisioning flexibility
- Service leveraging (mail filtering, information scanning, storage options (repl), security services)
- Hosting dynamics (mid term)
  - Periodic re-provisioning
  - Periodic re-hosting
  - Control mechanism rotation

Standards have more benefit in the Cloud

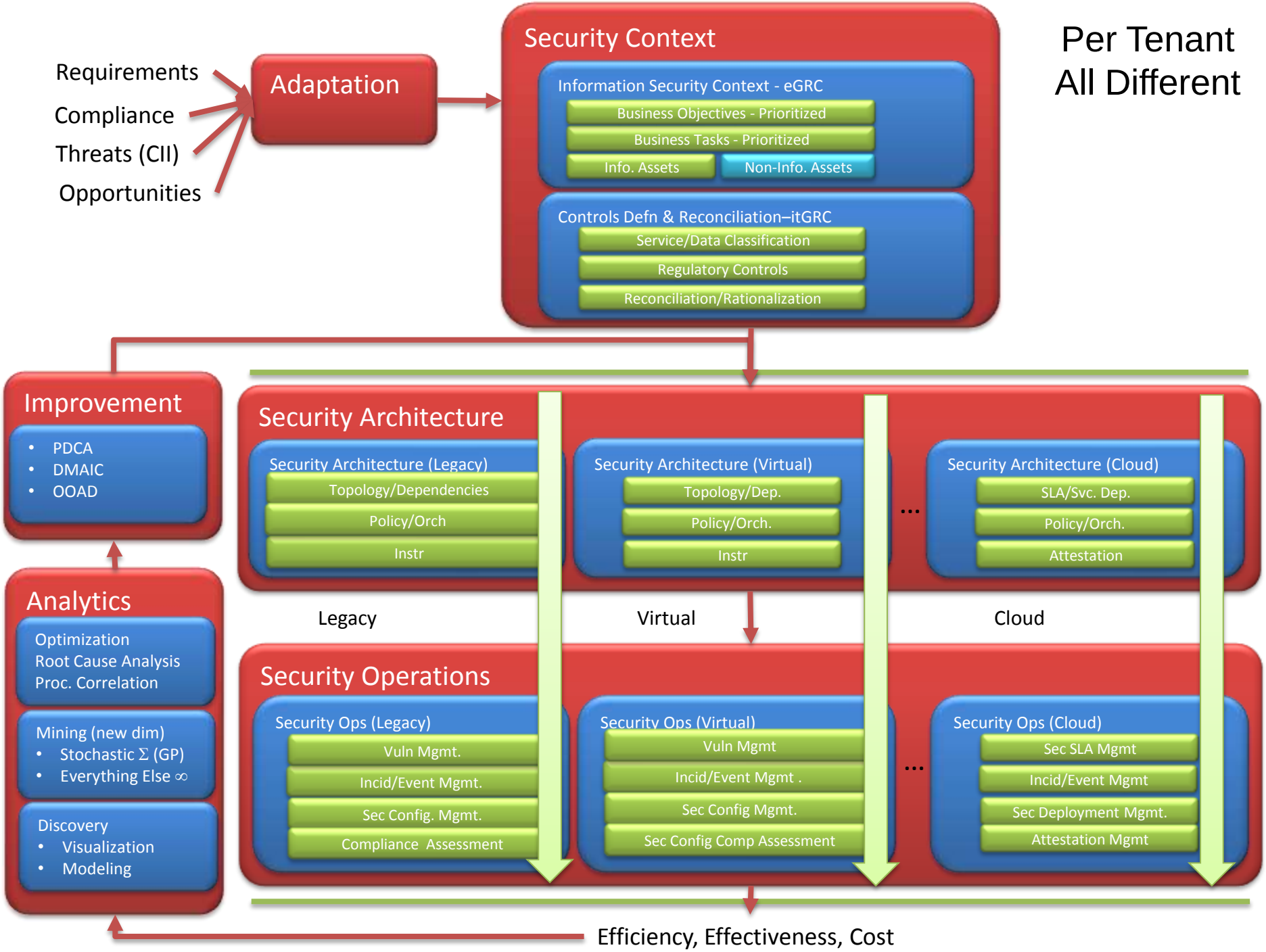
- Reduce ambiguity
- Normalize vocabulary
- Cloud source guidance - guidance
- Close the loop – measurement, effectiveness
- Share empirical feedback
- Community broader situation awareness
- ….

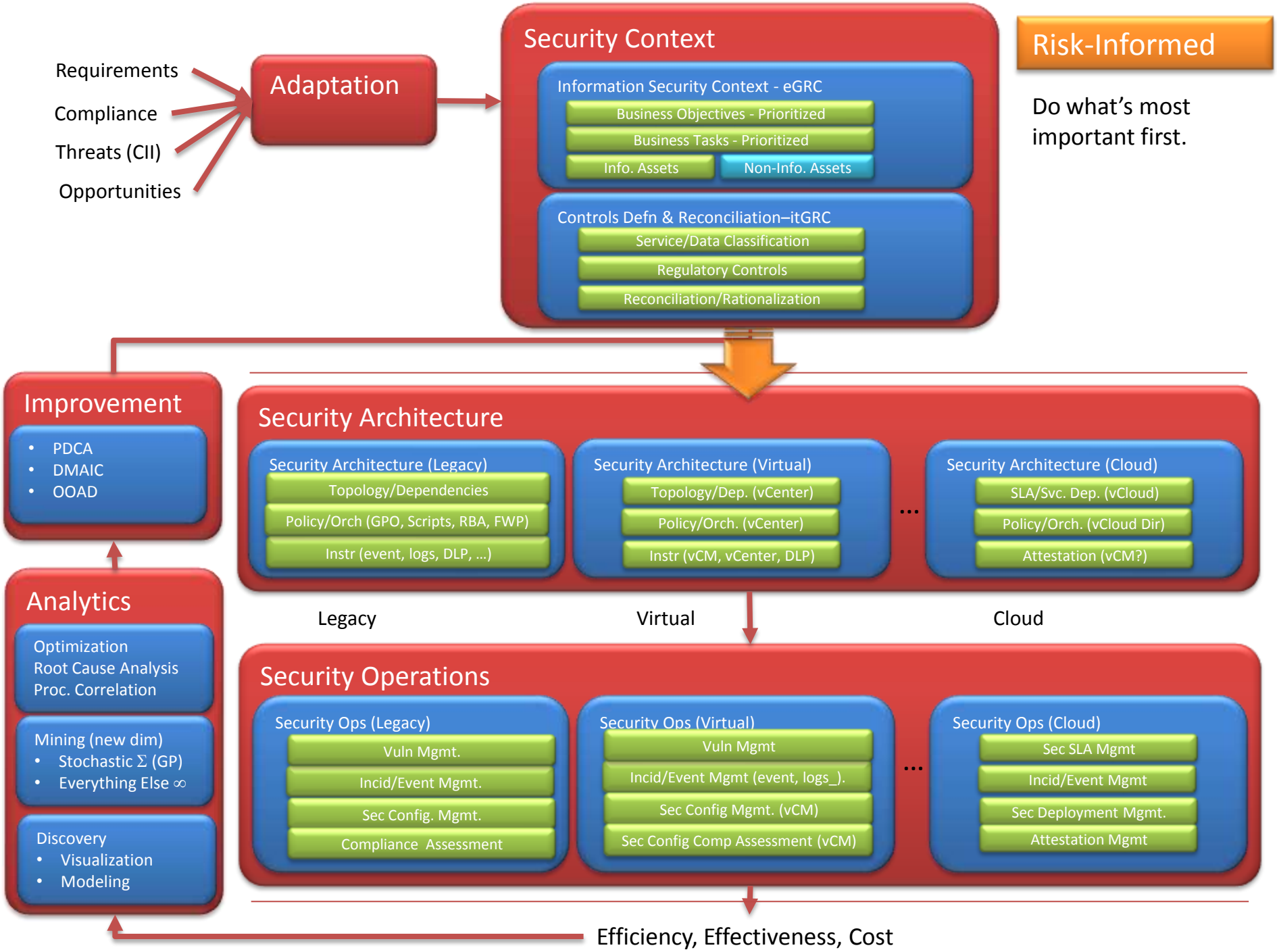
Automation: The Goal

- Automation doesn’t happen for it’s own sake:
- Objectives (increasing):
  - Efficiency - work per unit time
  - Efficacy - confirmation of result
  - Alignment - appropriate coherence
  - Improvement - refinement
  - Agility – alternatives
- But … Automation can create inertial mass (scripts)

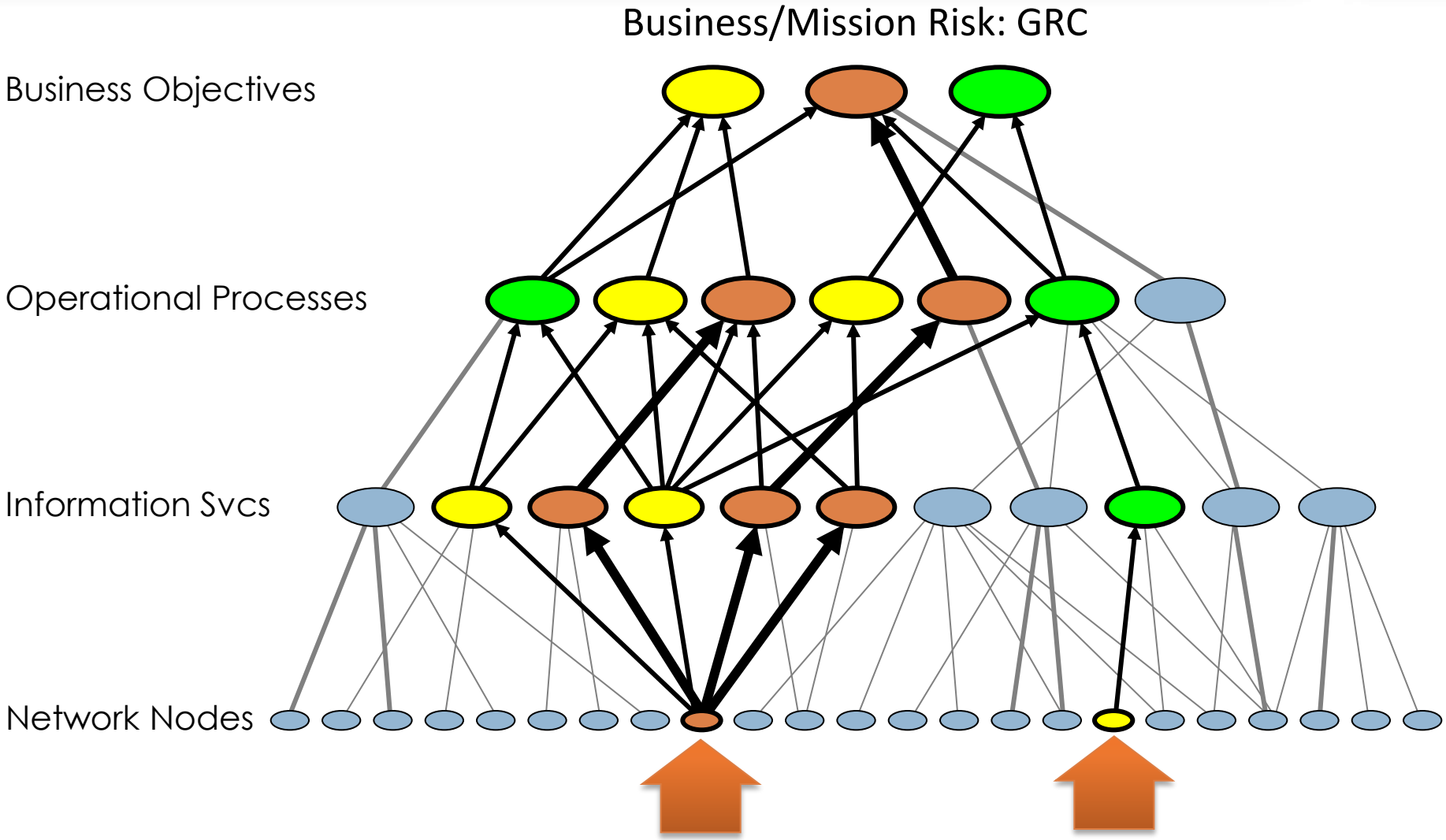
Good Automation

- Automation -> Efficiency
- += Feedback -> Alignment
- += Measurement -> Improvement
- += Analytics -> Agility


Per Tenant
All Different
Requirements
Compliance
Threats (CII)
Opportunities
Adaptation
Security Context
Information Security Context - eGRC
Business Objectives - Prioritized
Business Tasks - Prioritized
Info. Assets
Non-Info. Assets
Controls Defn & Reconciliation–itGRC
Service/Data Classification
Regulatory Controls
Reconciliation/Rationalization
Improvement
PDCA
DMAIC
OOAD
Analytics
Optimization
Root Cause Analysis
Proc. Correlation
Mining (new dim)
Stochastic Σ (GP)
Everything Else ∞
Discovery
Visualization
Modeling
Security Architecture
Security Architecture (Legacy)
Topology/Dependencies
Policy/Orch
Instr
Security Architecture (Virtual)
Topology/Dep.
Policy/Orch.
Instr
...
Security Architecture (Cloud)
SLA/Svc. Dep.
Policy/Orch.
Attestation
Legacy
Virtual
Cloud
Security Operations
Security Ops (Legacy)
Vuln Mgmt.
Incid/Event Mgmt.
Sec Config. Mgmt.
Compliance Assessment
Security Ops (Virtual)
Vuln Mgmt
Incid/Event Mgmt .
Sec Config Mgmt.
Sec Config Comp Assessment
...
Security Ops (Cloud)
Sec SLA Mgmt
Incid/Event Mgmt
Sec Deployment Mgmt.
Attestation Mgmt
Efficiency, Effectiveness, Cost


Requirements
Compliance
Threats (CII)
Opportunities
Adaptation
Security Context
Information Security Context - eGRC
Business Objectives - Prioritized
Business Tasks - Prioritized
Info. Assets
Non-Info. Assets
Controls Defn & Reconciliation–itGRC
Service/Data Classification
Regulatory Controls
Reconciliation/Rationalization
Risk-Informed
Do what's most important first.
Improvement
PDCA
DMAIC
OOAD
Analytics
Optimization
Root Cause Analysis
Proc. Correlation
Mining (new dim)
Stochastic Σ (GP)
Everything Else ∞
Discovery
Visualization
Modeling
Security Architecture
Security Architecture (Legacy)
Topology/Dependencies
Policy/Orch (GPO, Scripts, RBA, FWP)
Instr (event, logs, DLP, ...)
Security Architecture (Virtual)
Topology/Dep. (vCenter)
Policy/Orch. (vCenter)
Instr (vCM, vCenter, DLP)
...
Security Architecture (Cloud)
SLA/Svc. Dep. (vCloud)
Policy/Orch. (vCloud Dir)
Attestation (vCM?)
Legacy
Virtual
Cloud
Security Operations
Security Ops (Legacy)
Vuln Mgmt.
Incid/Event Mgmt.
Sec Config. Mgmt.
Compliance Assessment
Security Ops (Virtual)
Vuln Mgmt
Incid/Event Mgmt (event, logs_).
Sec Config Mgmt. (vCM)
Sec Config Comp Assessment (vCM)
...
Security Ops (Cloud)
Sec SLA Mgmt
Incid/Event Mgmt
Sec Deployment Mgmt.
Attestation Mgmt
Efficiency, Effectiveness, Cost

RISK CONTEXT



Automated Content: CVE, CVSS, CWE

RSA
The Security Division of EMC

Virtualization => More Coupling

Services

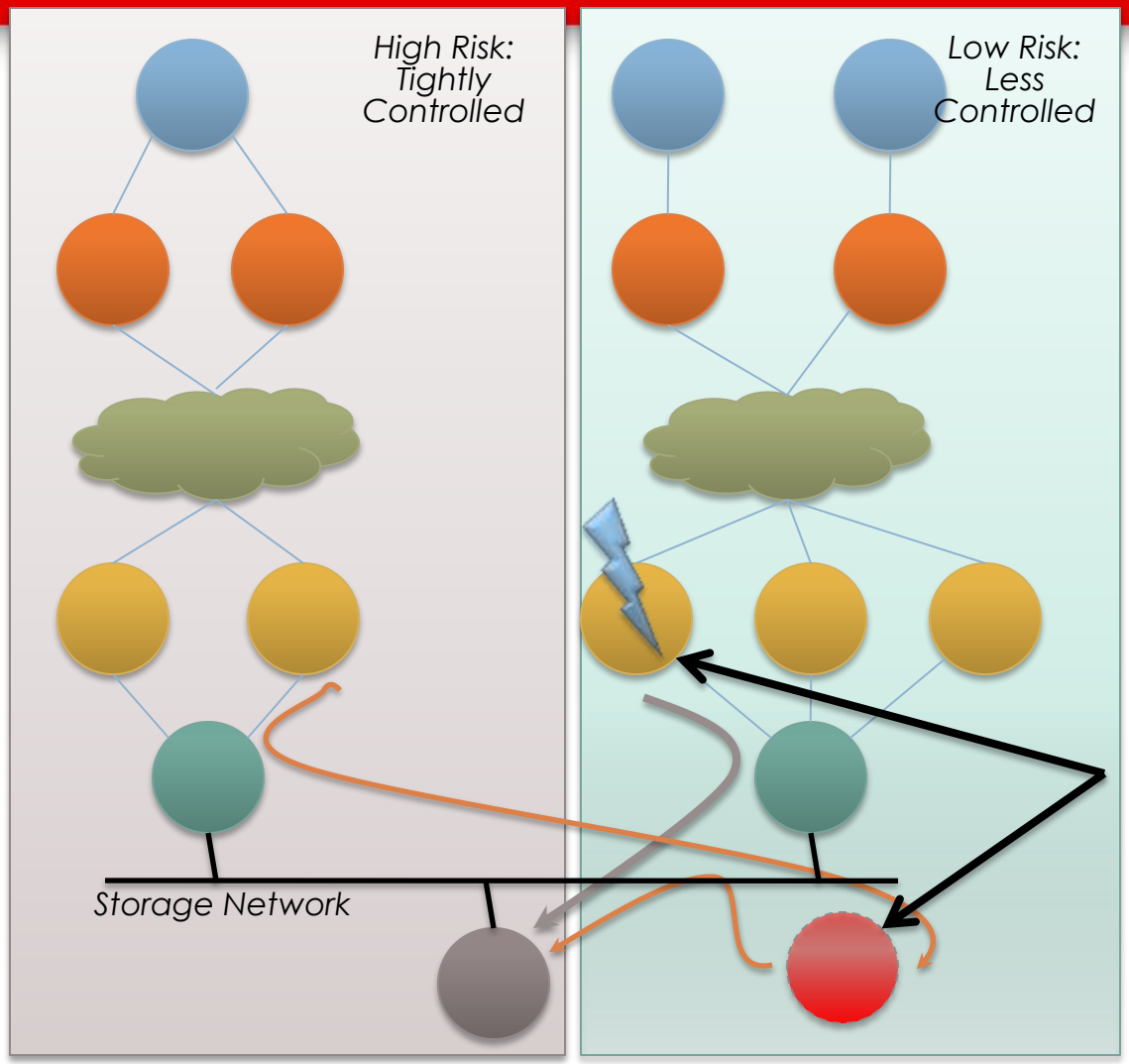
Applications

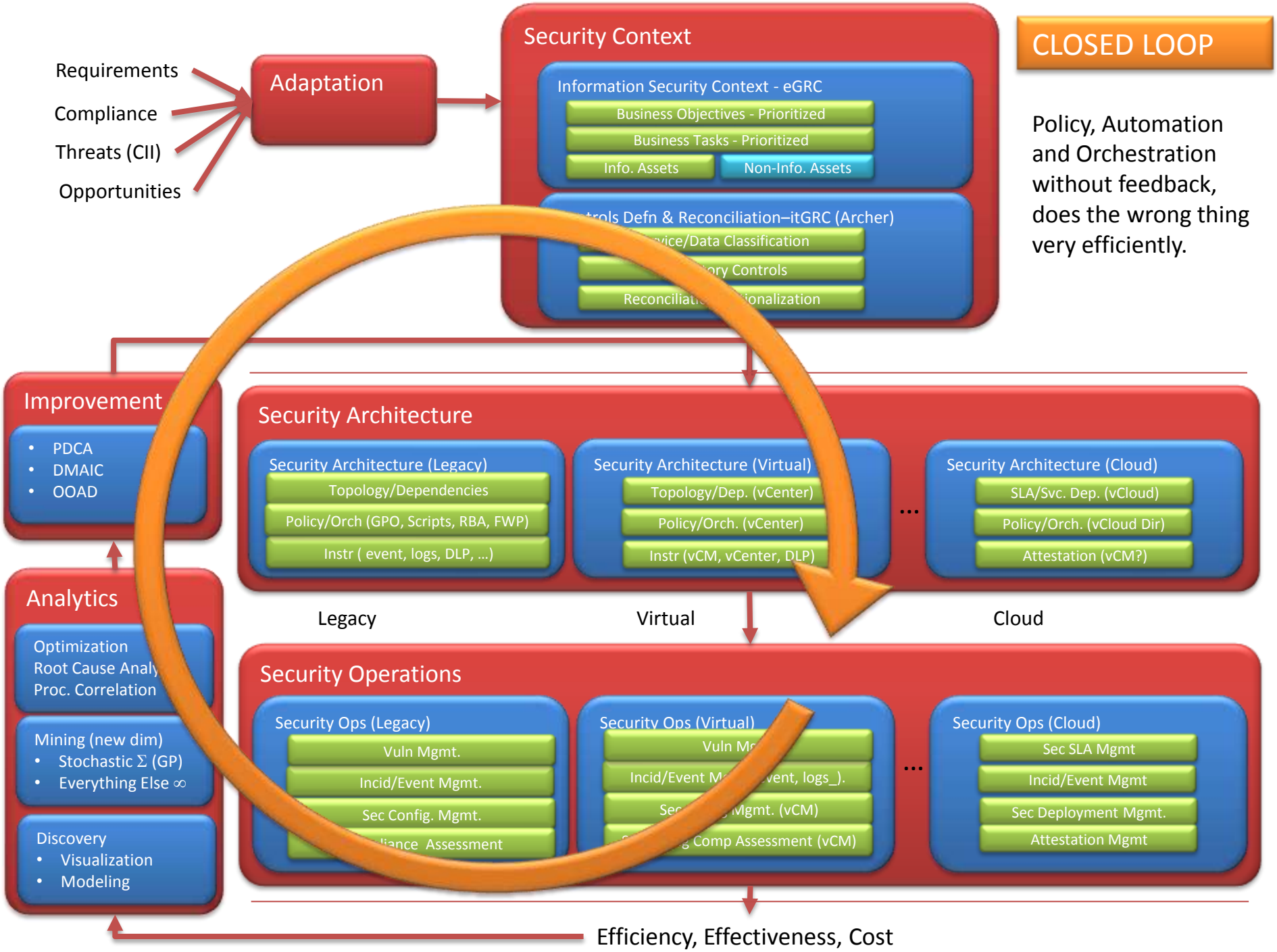
Network Virtualization

Virtualized Guests

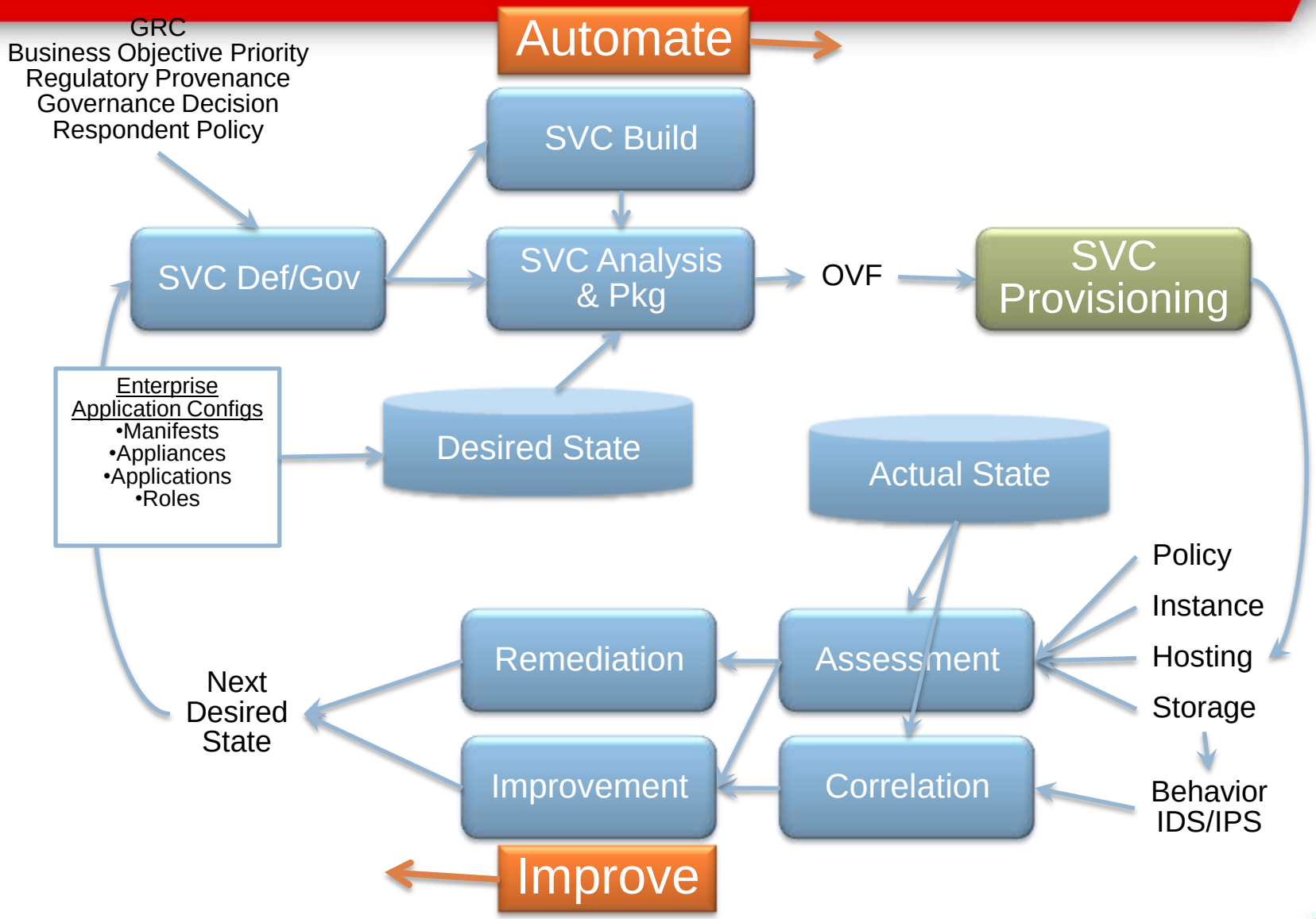
Virtualization Hosts

SAN - Storage Virtualization



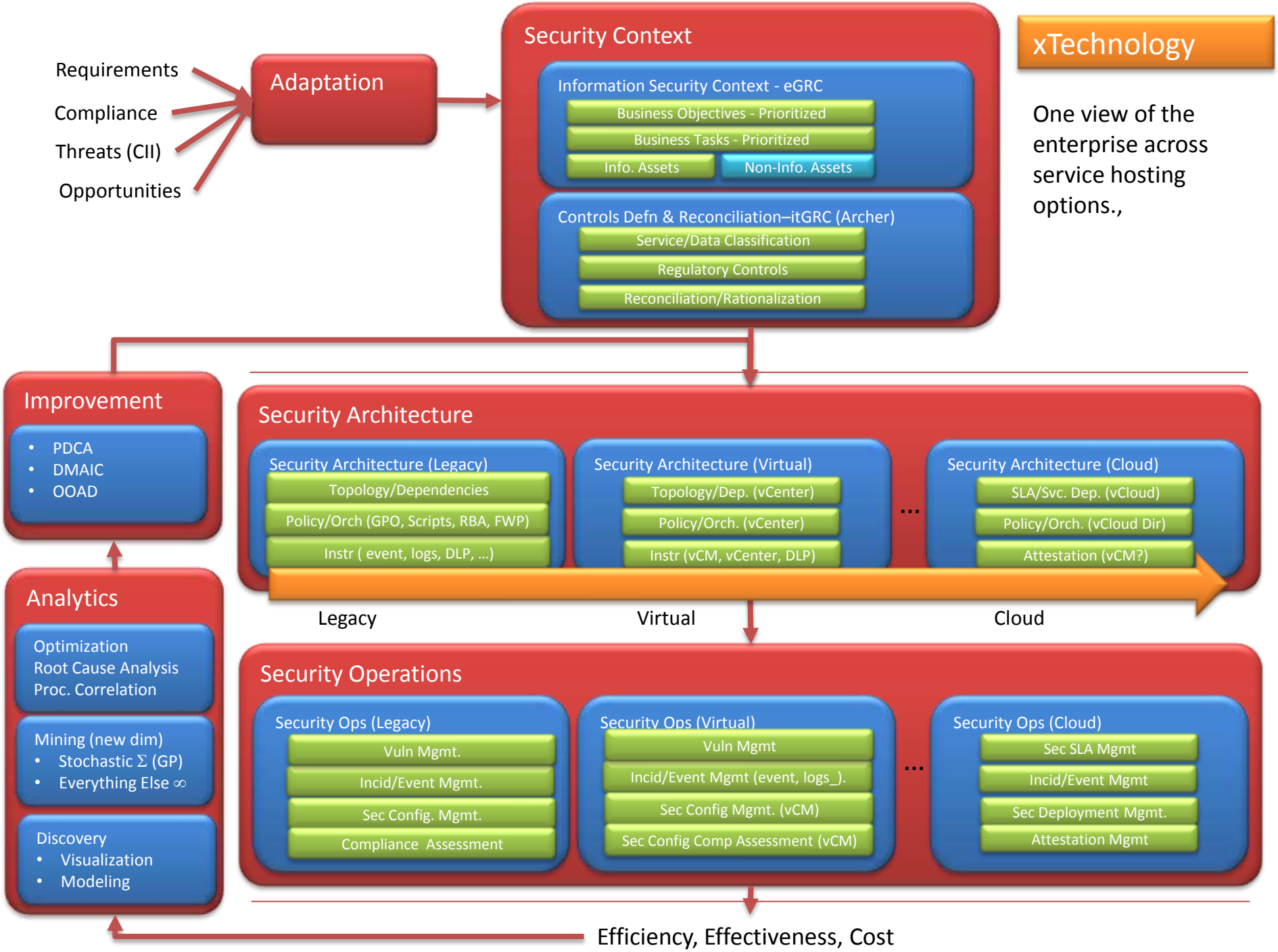

Requirements
Compliance
Threats (CII)
Opportunities
Adaptation
Security Context
Information Security Context - eGRC
Business Objectives - Prioritized
Business Tasks - Prioritized
Info. Assets
Non-Info. Assets
Defn & Reconciliation–itGRC (Archer)
Data Classification
Controls
Reconciliation
CLOSED LOOP
Policy, Automation and Orchestration without feedback, does the wrong thing very efficiently.
Improvement
PDCA
DMAIC
OOAD
Analytics
Optimization
Root Cause Analy
Proc. Correlation
Mining (new dim)
Stochastic Σ (GP)
Everything Else ∞
Discovery
Visualization
Modeling
Security Architecture
Security Architecture (Legacy)
Topology/Dependencies
Policy/Orch (GPO, Scripts, RBA, FWP)
Instr (event, logs, DLP, ...)
Security Architecture (Virtual)
Topology/Dep. (vCenter)
Policy/Orch. (vCenter)
Instr (vCM, vCenter, DLP)
...
Security Architecture (Cloud)
SLA/Svc. Dep. (vCloud)
Policy/Orch. (vCloud Dir)
Attestation (vCM?)
Legacy
Virtual
Cloud
Security Operations
Security Ops (Legacy)
Vuln Mgmt.
Incid/Event Mgmt.
Sec Config. Mgmt.
Security Ops (Virtual)
Comp Assessment (vCM)
...
Security Ops (Cloud)
Sec SLA Mgmt
Incid/Event Mgmt
Sec Deployment Mgmt.
Attestation Mgmt
Efficiency, Effectiveness, Cost

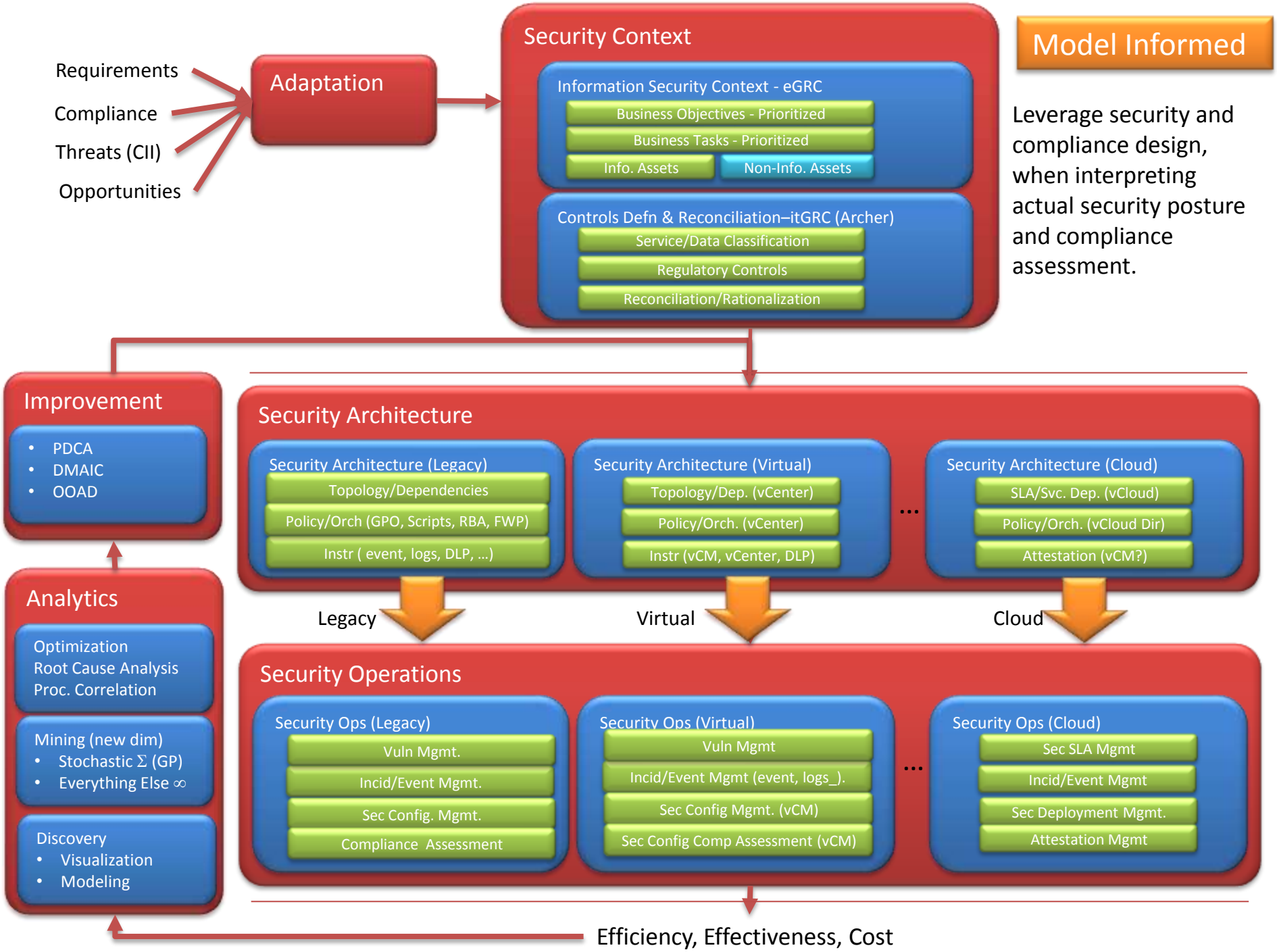
Operations Cycle



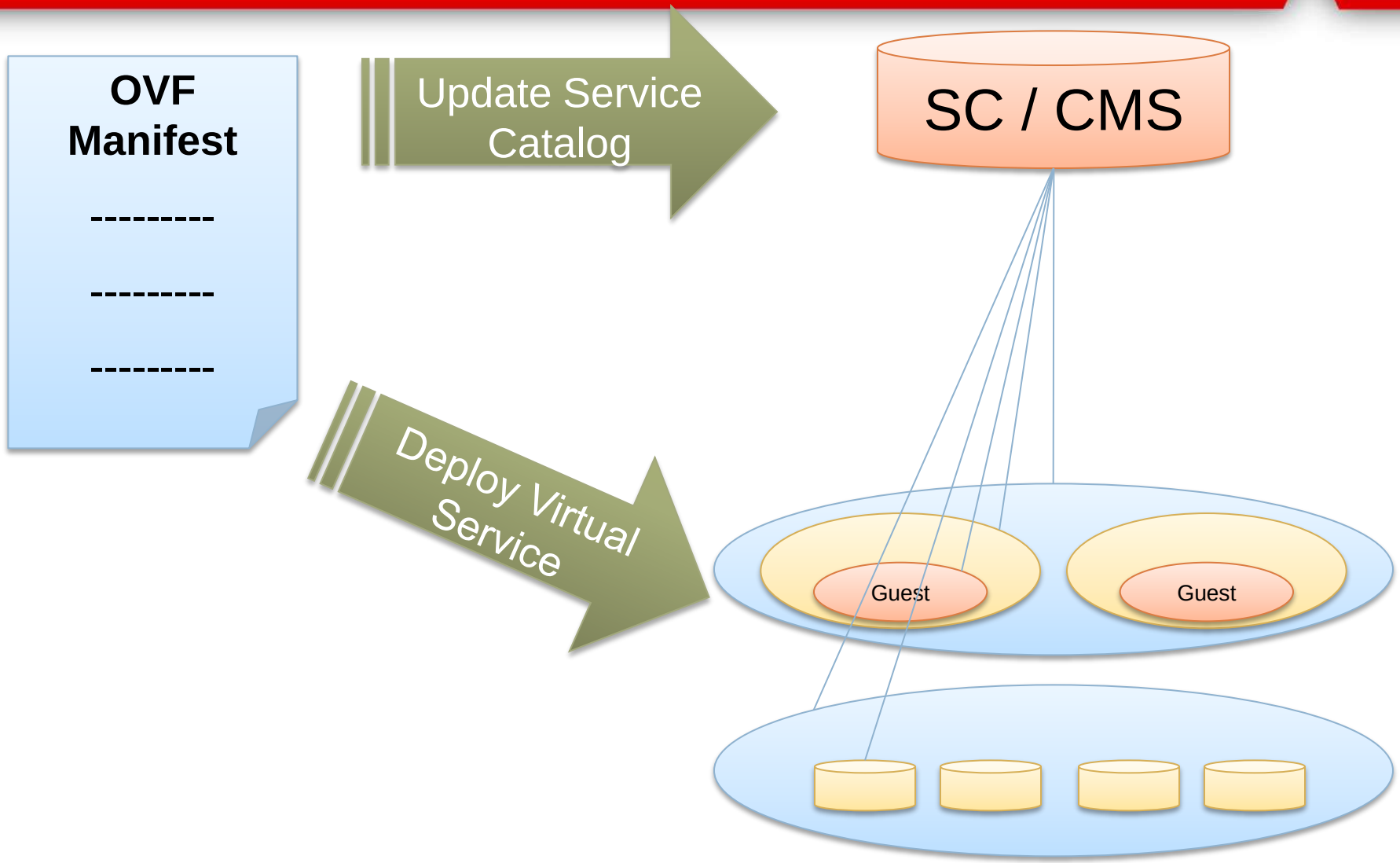
Automated Content: OVAL, CVE, CVSS, CWE, …

RSA
The Security Division of EMC


Requirements
Compliance
Threats (CII)
Opportunities
Adaptation
Security Context
Information Security Context - eGRC
Business Objectives - Prioritized
Business Tasks - Prioritized
Info. Assets
Non-Info. Assets
Controls Defn & Reconciliation–itGRC (Archer)
Service/Data Classification
Regulatory Controls
Reconciliation/Rationalization
xTechnology
One view of the enterprise across service hosting options.,
Improvement
PDCA
DMAIC
OOAD
Analytics
Optimization
Root Cause Analysis
Proc. Correlation
Mining (new dim)
Stochastic Σ (GP)
Everything Else ∞
Discovery
Visualization
Modeling
Security Architecture
Security Architecture (Legacy)
Topology/Dependencies
Policy/Orch (GPO, Scripts, RBA, FWP)
Instr (event, logs, DLP, ...)
Security Architecture (Virtual)
Topology/Dep. (vCenter)
Policy/Orch. (vCenter)
Instr (vCM, vCenter, DLP)
...
Security Architecture (Cloud)
SLA/Svc. Dep. (vCloud)
Policy/Orch. (vCloud Dir)
Attestation (vCM?)
Legacy
Virtual
Cloud
Security Operations
Security Ops (Legacy)
Vuln Mgmt.
Incid/Event Mgmt.
Sec Config. Mgmt.
Compliance Assessment
Security Ops (Virtual)
Vuln Mgmt
Incid/Event Mgmt (event, logs_).
Sec Config Mgmt. (vCM)
Sec Config Comp Assessment (vCM)
...
Security Ops (Cloud)
Sec SLA Mgmt
Incid/Event Mgmt
Sec Deployment Mgmt.
Attestation Mgmt
Efficiency, Effectiveness, Cost


Requirements
Compliance
Threats (CII)
Opportunities
Adaptation
Security Context
Information Security Context - eGRC
Business Objectives - Prioritized
Business Tasks - Prioritized
Info. Assets
Non-Info. Assets
Controls Defn & Reconciliation–itGRC (Archer)
Service/Data Classification
Regulatory Controls
Reconciliation/Rationalization
Model Informed
Leverage security and compliance design, when interpreting actual security posture and compliance assessment.
Improvement
PDCA
DMAIC
OOAD
Analytics
Optimization
Root Cause Analysis
Proc. Correlation
Mining (new dim)
Stochastic Σ (GP)
Everything Else ∞
Discovery
Visualization
Modeling
Security Architecture
Security Architecture (Legacy)
Topology/Dependencies
Policy/Orch (GPO, Scripts, RBA, FWP)
Instr (event, logs, DLP, ...)
Security Architecture (Virtual)
Topology/Dep. (vCenter)
Policy/Orch. (vCenter)
Instr (vCM, vCenter, DLP)
...
Security Architecture (Cloud)
SLA/Svc. Dep. (vCloud)
Policy/Orch. (vCloud Dir)
Attestation (vCM?)
Legacy
Virtual
Cloud
Security Operations
Security Ops (Legacy)
Vuln Mgmt.
Incid/Event Mgmt.
Sec Config. Mgmt.
Compliance Assessment
Security Ops (Virtual)
Vuln Mgmt
Incid/Event Mgmt (event, logs_).
Sec Config Mgmt. (vCM)
Sec Config Comp Assessment (vCM)
...
Security Ops (Cloud)
Sec SLA Mgmt
Incid/Event Mgmt
Sec Deployment Mgmt.
Attestation Mgmt
Efficiency, Effectiveness, Cost

Service Model: OVF



RSA
The Security Division of EMC

Service Model: OVF

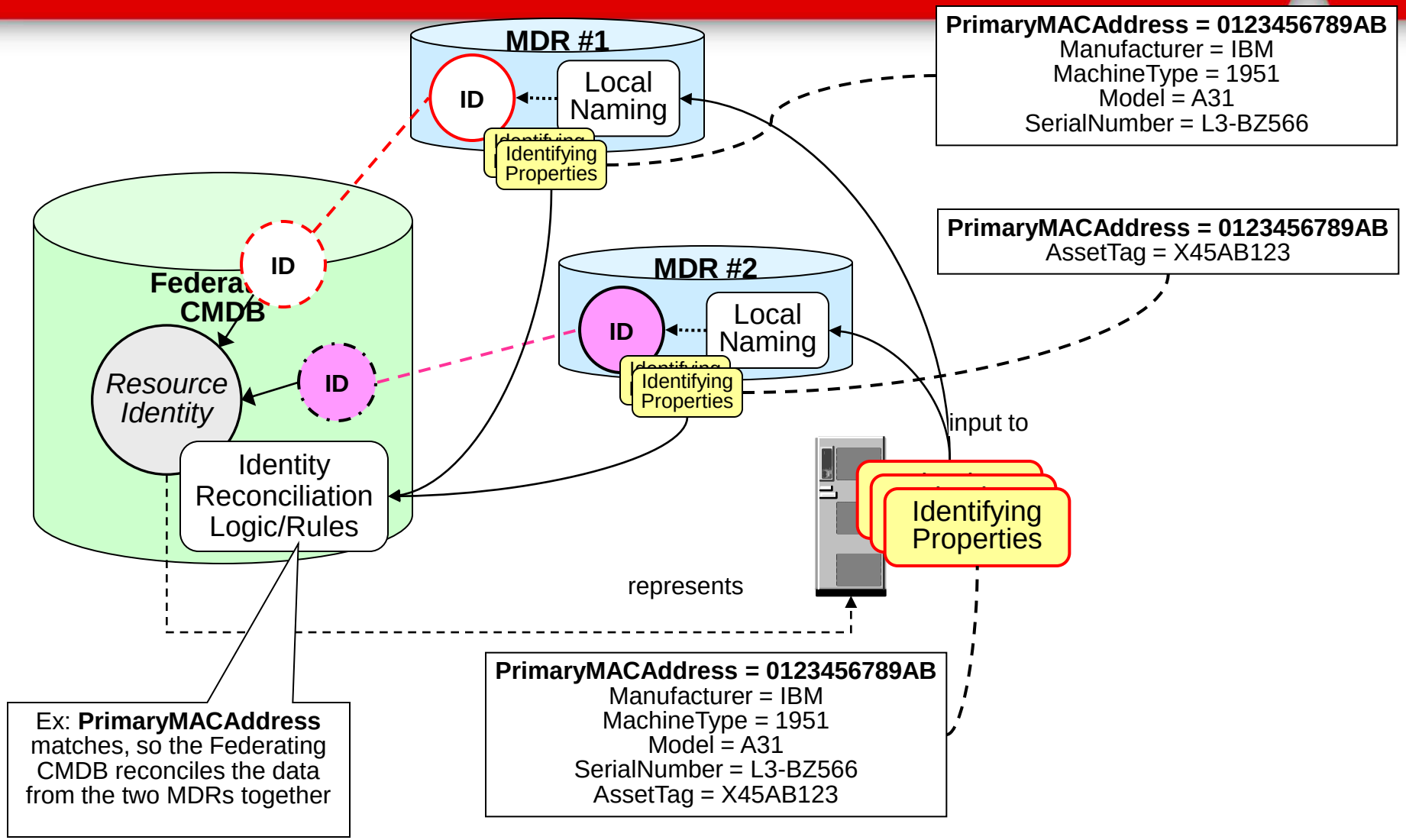
App Server

DB Server

```
</ProductSection>
- <StartupSection>
  <Info>Startup order of the virtual machines</Info>
  <Item ovf:id="DBServer" ovf:order="1" ovf:startDelay="120" ovf:startAction="powerOn" ovf:waitingForGuest="true"
  <Item ovf:id="AppServer" ovf:order="2" ovf:startDelay="120" ovf:startAction="powerOn" ovf:waitingForGuest="true"
  </StartupSection>

- <VirtualSystem ovf:id="AppServer">
  <Info>The configuration of the AppServer virtual m
  <Name>Application Server</Name>
- <!-- Linux component configuration parameters   -->
- <ProductSection ovf:class="org.linuxdist.x">
  <Info>Product customization for the installed Linu
  <Product>Linux Distribution X</Product>
  <Version>2.6.3</Version>
  <Property ovf:key="hostname" ovf:type="string" ovf
  <Property ovf:key="ip" ovf:type="string" ovf:value="$
  <Property ovf:key="subnet" ovf:type="string" ovf:val
…
  </ProductSection>
- <OperatingSystemSection ovf:id="36">
  <Info>Guest Operating System</Info>
  <Description>Linux 2.6.x</Description>
  </OperatingSystemSection>
- <VirtualHardwareSection>
  <Info>Virtual Hardware Requirements: 256 MB, 1 (
…
- <Item>
  <rasd:Description>Number of virtual CPUs</rasd:D
  <rasd:ElementName>1 virtual CPU</rasd:ElementN
…
```

```
- <VirtualSystem ovf:id="DBServer">
  <Info>The configuration of the database virtual machine</Info>
  <Name>Database Server</Name>
- <!-- Linux component configuration parameters   -->
- <ProductSection ovf:class="org.linuxdist.x">
  <Info>Product customization for the installed Linux system</Info>
  <Product>Linux Distribution X</Product>
  <Version>2.6.3</Version>
  <Property ovf:key="hostname" ovf:type="string" ovf:value="${dbHostname}" />
  <Property ovf:key="ip" ovf:type="string" ovf:value="${dbIp}" />
  <Property ovf:key="subnet" ovf:type="string" ovf:value="${subnet}" />
…
  </ProductSection>
- <OperatingSystemSection ovf:id="36">
  <Info>Guest Operating System</Info>
  <Description>Linux 2.6.x</Description>
  </OperatingSystemSection>
- <VirtualHardwareSection>
  <Info>Virtual Hardware Requirements: 256 MB, 1 CPU, 1 disk, 1 nic</Info>
…
- <Item>
  <rasd:Description>Number of virtual CPUs</rasd:Description>
  <rasd:ElementName>1 virtual CPU</rasd:ElementName>
…
```

Asset Model: CMDB (ITIL), CMDBf (DMTF)

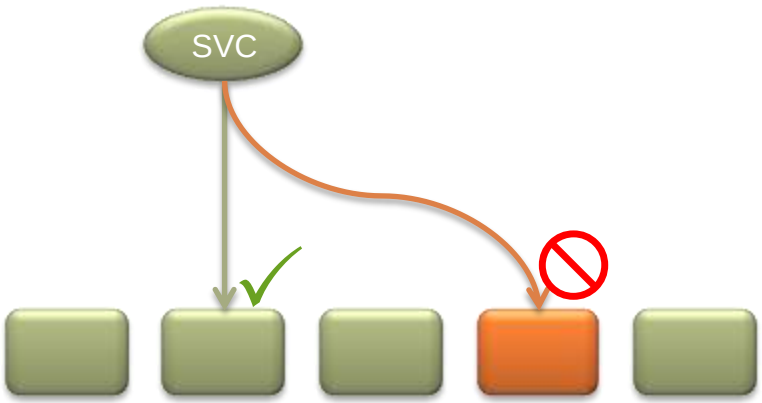


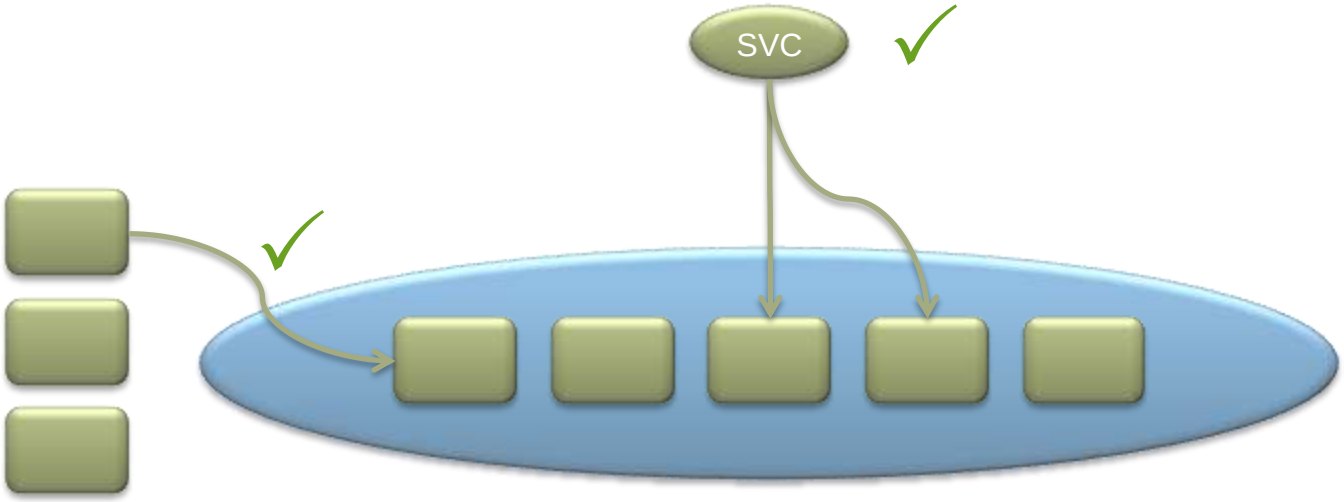
Leveraging a CMDB

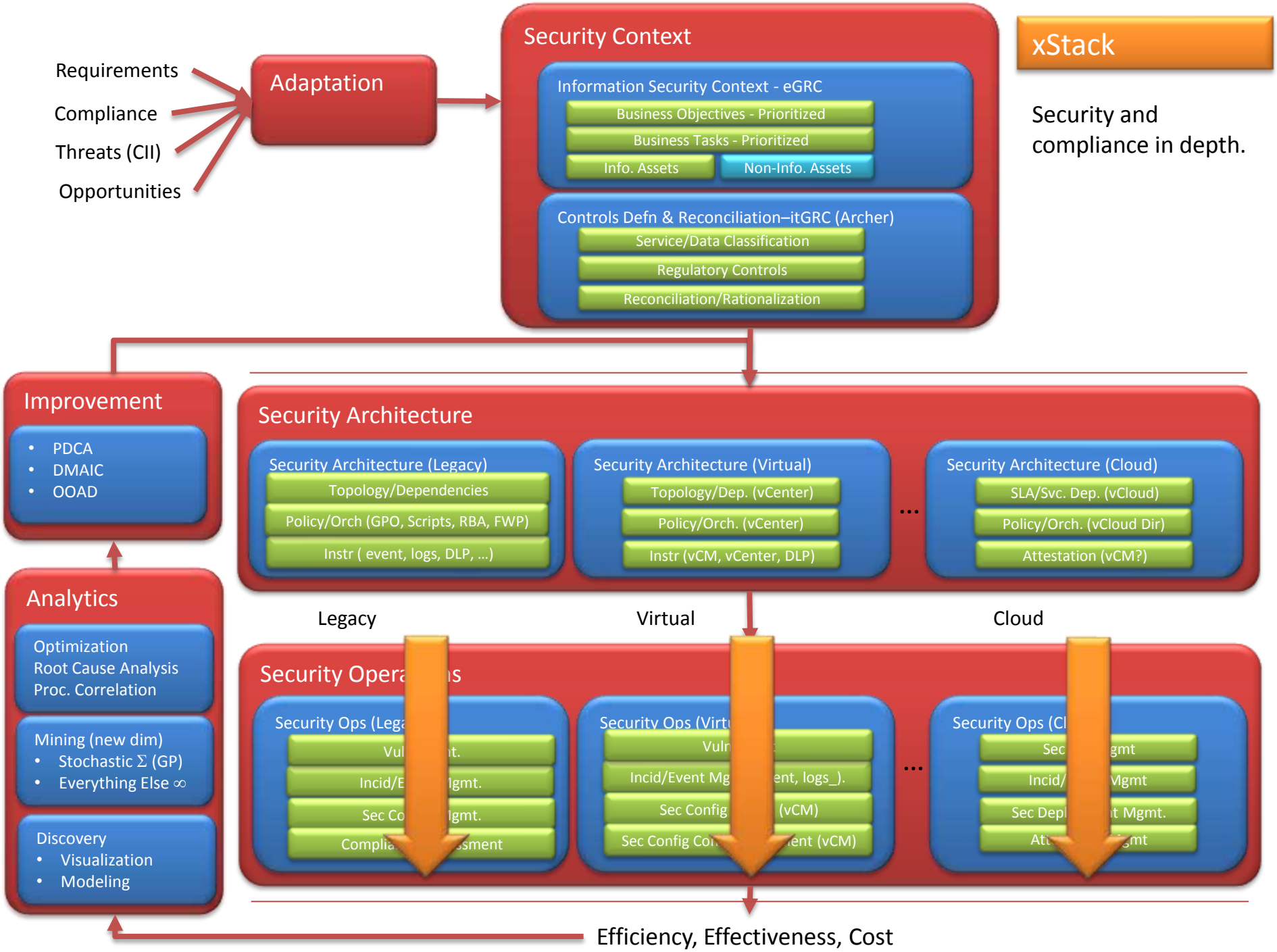
```
<query>
  <itemTemplate id="user">
    <recordConstraint>
      <recordType namespace="http://example.com/people" localName="person"/>
      <propertyValue namespace="http://example.com/people" localName="state">
        <equal>CA</equal>
      </propertyValue>
    </recordConstraint>
  </itemTemplate>

  <itemTemplate id="computer">
    <recordConstraint>
      <recordType namespace="http://example.com/computer" localName="computer"/>
    </recordConstraint>
  </itemTemplate>

  <relationshipTemplate id="usage">
    <recordConstraint>
      <recordType namespace="http://example.co
    </recordConstraint>
    <targetTemplate ref="computer"/>
    <sourceTemplate ref="user"/>
  </relationshipTemplate>
</query>
```

- itemTemplate "user" selects a set of users
- itemTemplate "computer" selects a set of computers
- relationshipTemplate "usage" selects items that have a "uses" relationship from an item in "user" to an item in "computer" and returns these items and relationships

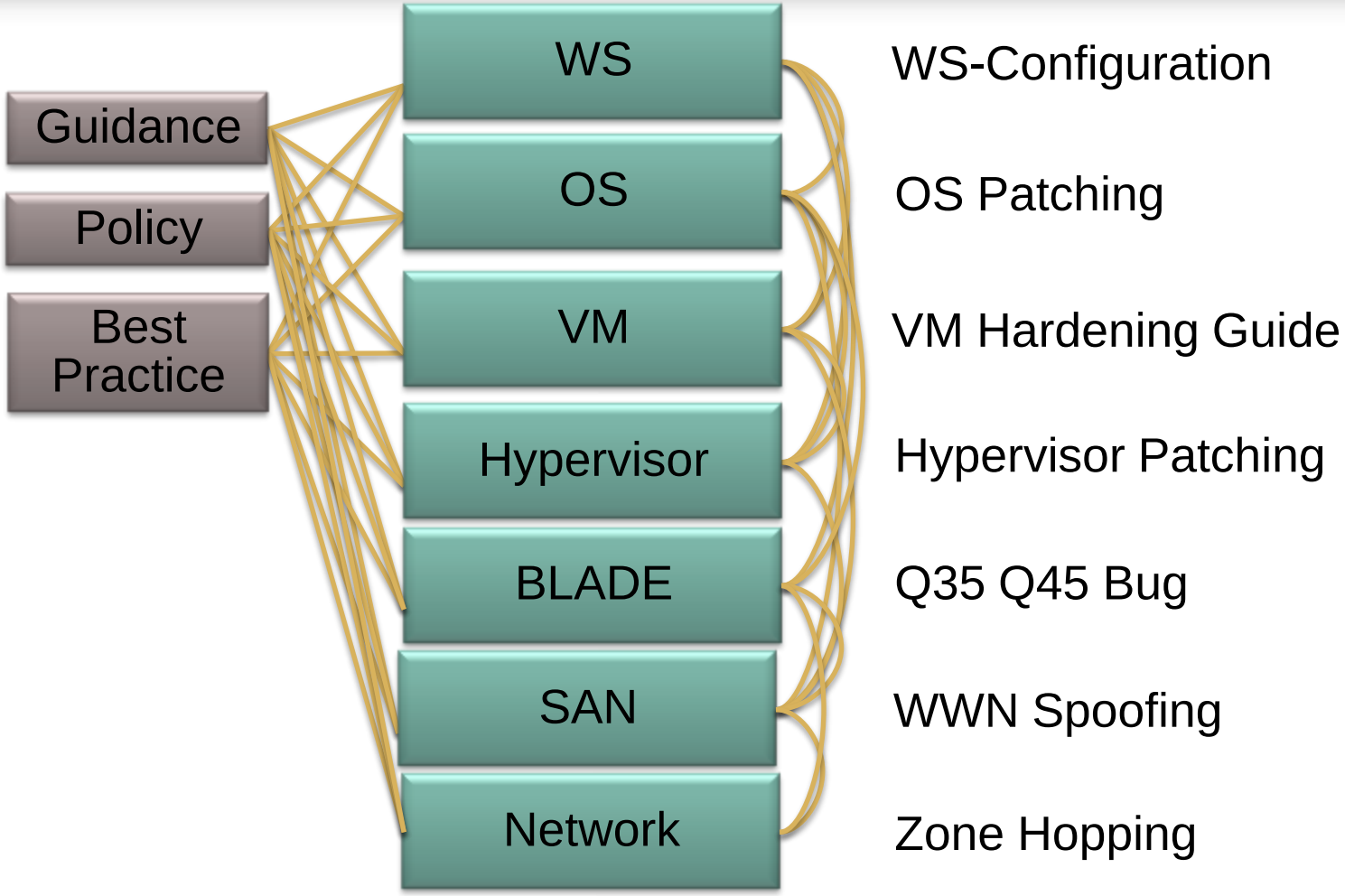
Provisioning Model: Leveraging Dynamics






Requirements
Compliance
Threats (CII)
Opportunities
Adaptation
Security Context
Information Security Context - eGRC
Business Objectives - Prioritized
Business Tasks - Prioritized
Info. Assets
Non-Info. Assets
Controls Defn & Reconciliation–itGRC (Archer)
Service/Data Classification
Regulatory Controls
Reconciliation/Rationalization
xStack
Security and compliance in depth.
Improvement
PDCA
DMAIC
OOAD
Analytics
Optimization
Root Cause Analysis
Proc. Correlation
Mining (new dim)
Stochastic Σ (GP)
Everything Else ∞
Discovery
Visualization
Modeling
Security Architecture
Security Architecture (Legacy)
Topology/Dependencies
Policy/Orch (GPO, Scripts, RBA, FWP)
Instr (event, logs, DLP, ...)
Security Architecture (Virtual)
Topology/Dep. (vCenter)
Policy/Orch. (vCenter)
Instr (vCM, vCenter, DLP)
...
Security Architecture (Cloud)
SLA/Svc. Dep. (vCloud)
Policy/Orch. (vCloud Dir)
Attestation (vCM?)
Legacy
Virtual
Cloud
Security Opera ns
Security Ops (Lega
Vul t.
Incid/E lgmt.
Sec Co lgmt.
Compli ssment
Security Ops (Virt
Vuln
Incid/Event Mg ent, logs_).
Sec Config (vCM)
Sec Config Co ent (vCM)
...
Security Ops (Cl
Sec gmt
Incid/ Mgmt
Sec Dep t Mgmt.
Att mt
Efficiency, Effectiveness, Cost

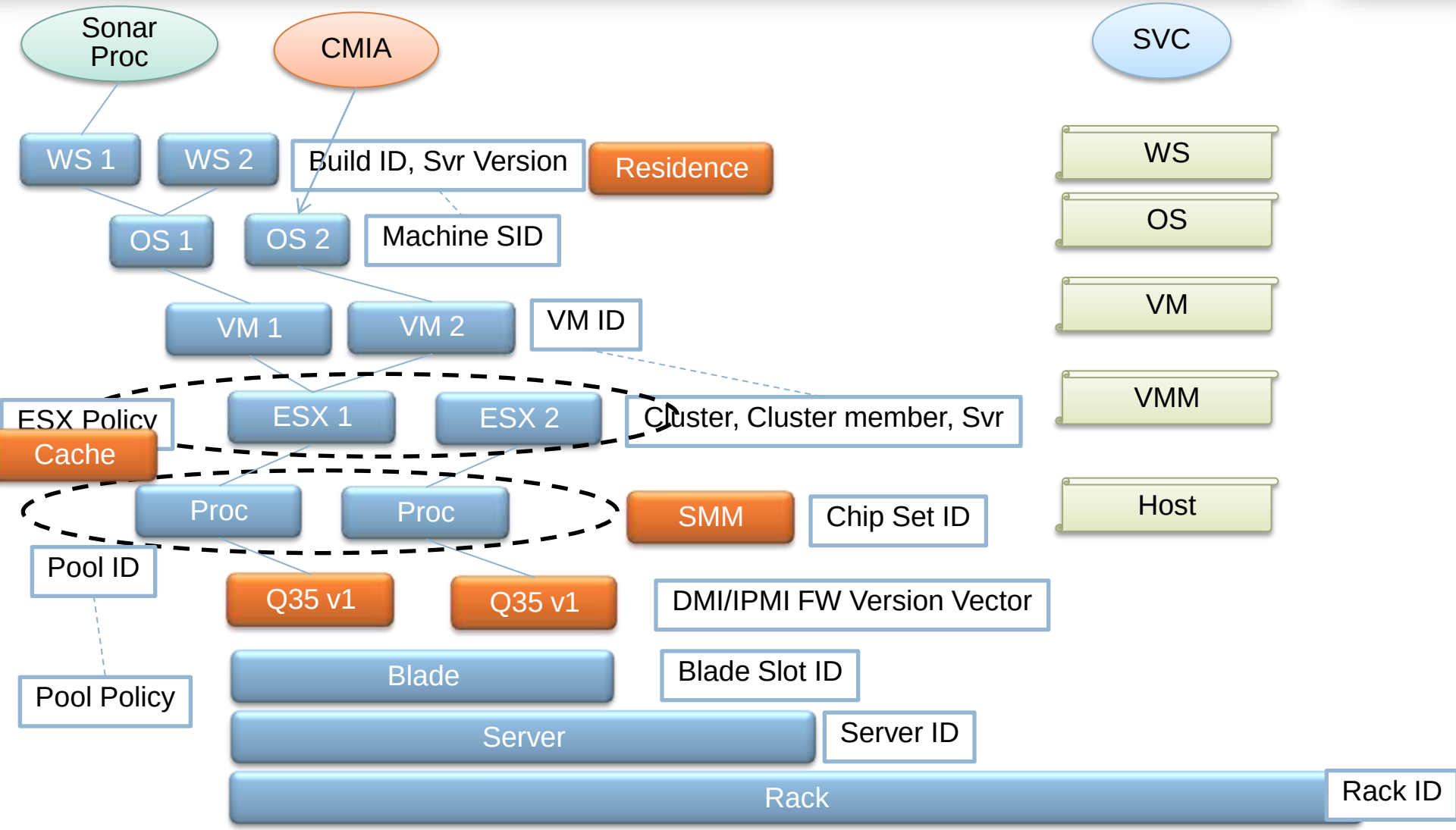
Security Across the Stack

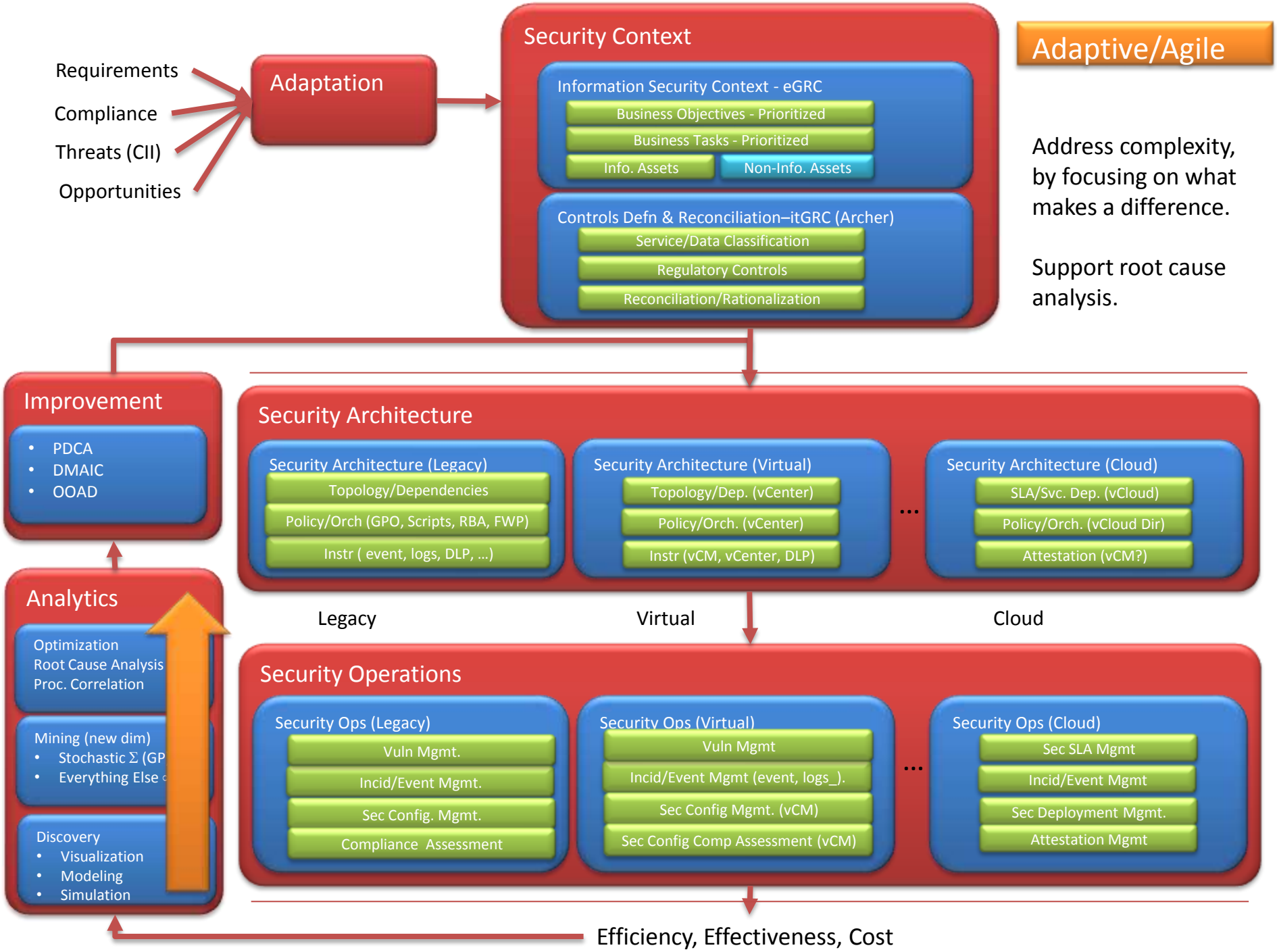


Automated Content: XCCDF, OVAL, CPE, CCE, OCIL

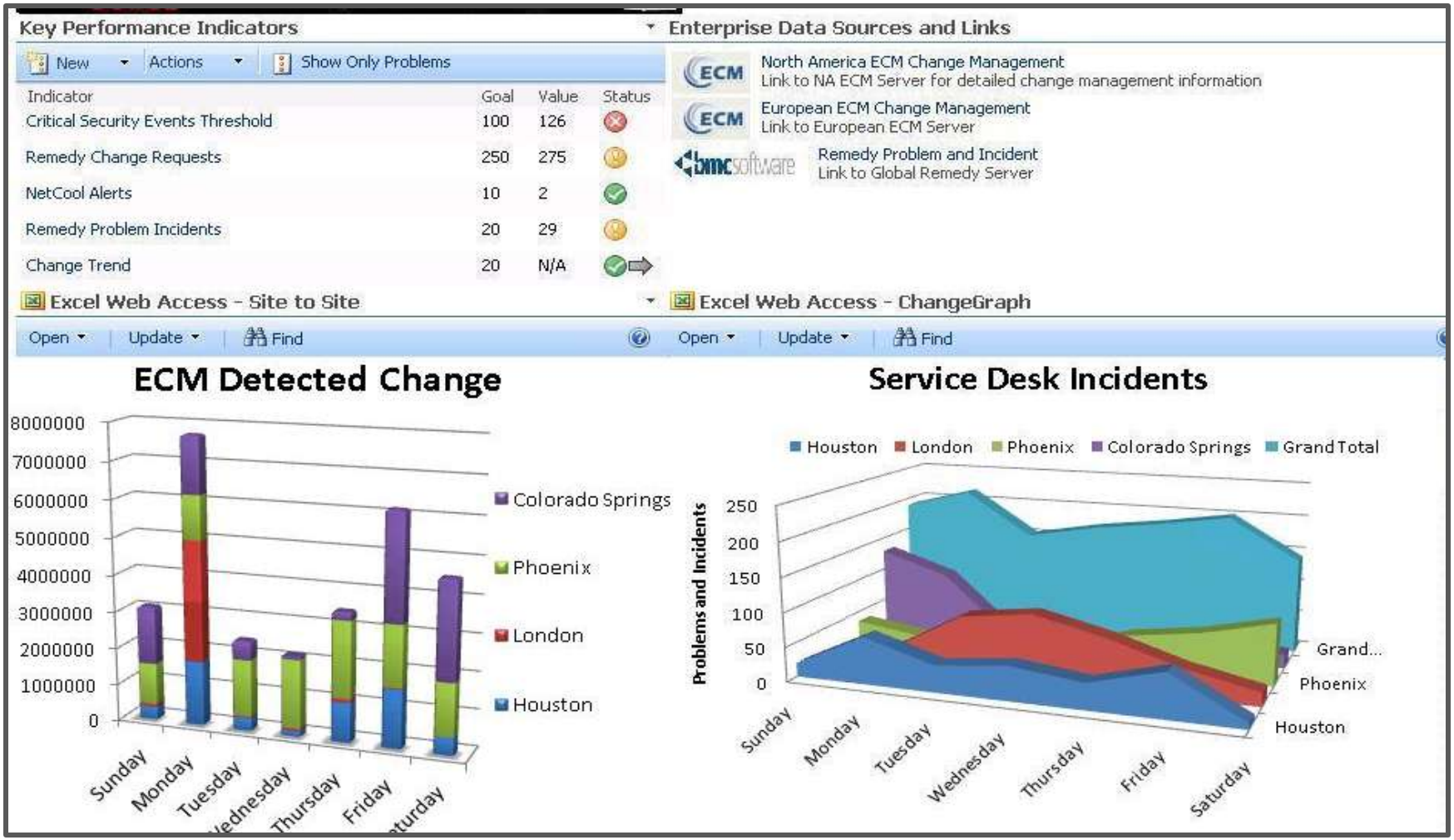
RSA
The Security Division of EMC

Security Coupling

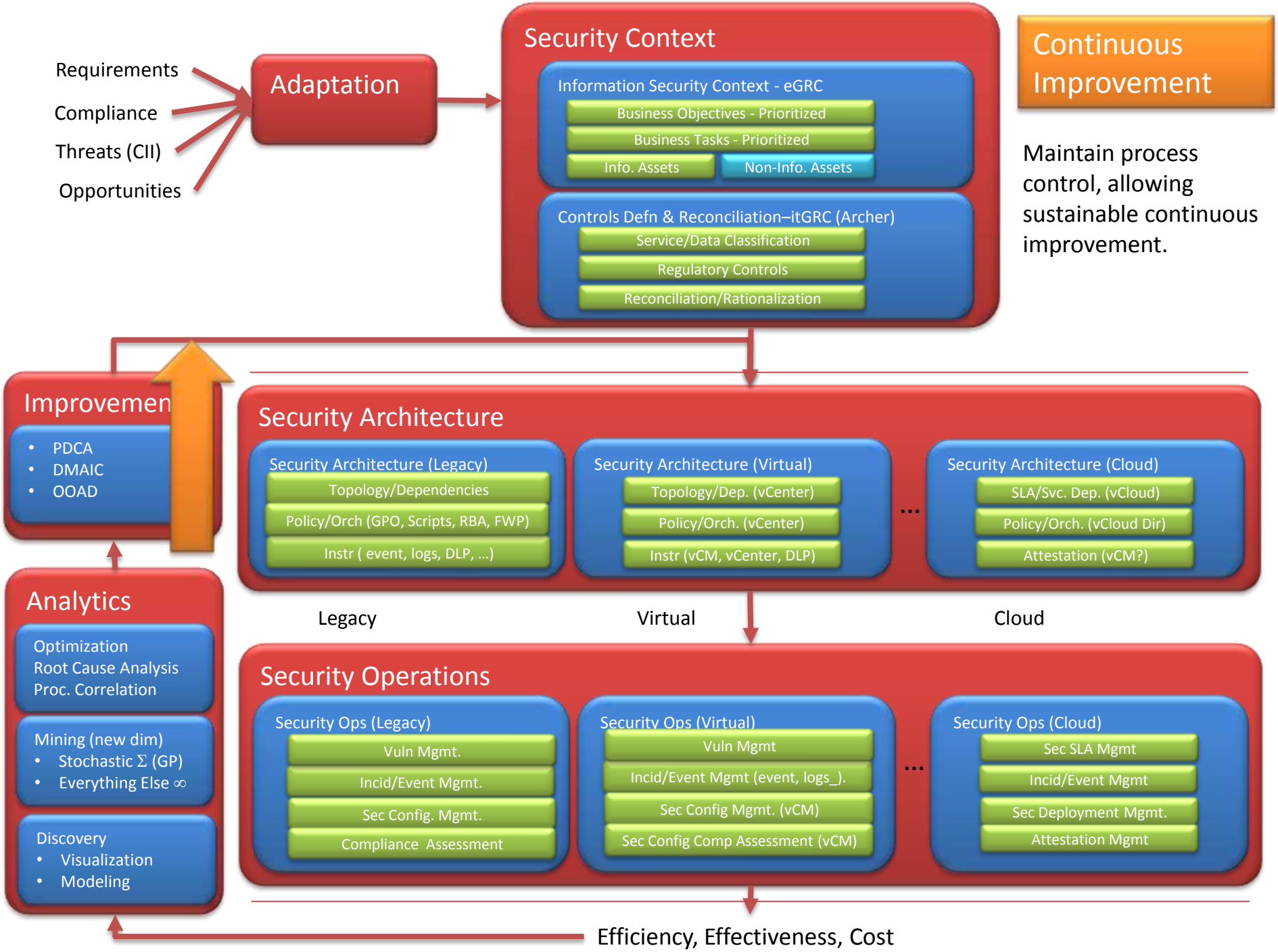



Requirements
Compliance
Threats (CII)
Opportunities
Adaptation
Security Context
Information Security Context - eGRC
Business Objectives - Prioritized
Business Tasks - Prioritized
Info. Assets
Non-Info. Assets
Controls Defn & Reconciliation–itGRC (Archer)
Service/Data Classification
Regulatory Controls
Reconciliation/Rationalization
Adaptive/Agile
Address complexity, by focusing on what makes a difference.
Support root cause analysis.
Improvement
PDCA
DMAIC
OOAD
Security Architecture
Security Architecture (Legacy)
Topology/Dependencies
Policy/Orch (GPO, Scripts, RBA, FWP)
Instr (event, logs, DLP, ...)
Security Architecture (Virtual)
Topology/Dep. (vCenter)
Policy/Orch. (vCenter)
Instr (vCM, vCenter, DLP)
...
Security Architecture (Cloud)
SLA/Svc. Dep. (vCloud)
Policy/Orch. (vCloud Dir)
Attestation (vCM?)
Legacy
Virtual
Cloud
Analytics
Optimization
Root Cause Analysis
Proc. Correlation
Mining (new dim)
Stochastic Σ (GP
Everything Else
Discovery
Visualization
Modeling
Simulation
Security Operations
Security Ops (Legacy)
Vuln Mgmt.
Incid/Event Mgmt.
Sec Config. Mgmt.
Compliance Assessment
Security Ops (Virtual)
Vuln Mgmt
Incid/Event Mgmt (event, logs_).
Sec Config Mgmt. (vCM)
Sec Config Comp Assessment (vCM)
...
Security Ops (Cloud)
Sec SLA Mgmt
Incid/Event Mgmt
Sec Deployment Mgmt.
Attestation Mgmt
Efficiency, Effectiveness, Cost

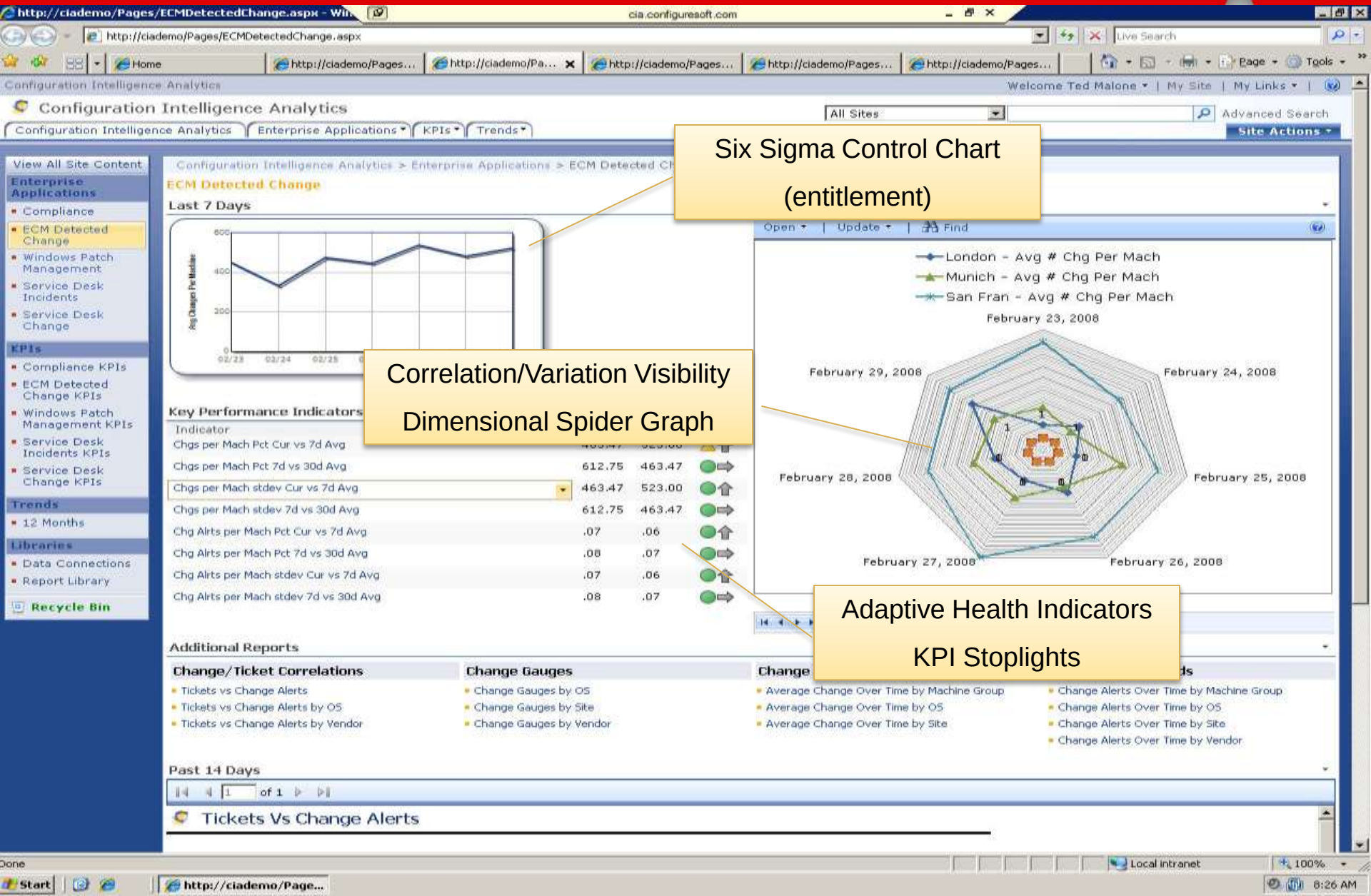
AGILTY: Situation Awareness



RSA
The Security Division of EMC


Requirements
Compliance
Threats (CII)
Opportunities
Adaptation
Security Context
Information Security Context - eGRC
Business Objectives - Prioritized
Business Tasks - Prioritized
Info. Assets
Non-Info. Assets
Controls Defn & Reconciliation–itGRC (Archer)
Service/Data Classification
Regulatory Controls
Reconciliation/Rationalization
Continuous Improvement
Maintain process control, allowing sustainable continuous improvement.
Improvemen
PDCA
DMAIC
OOAD
Security Architecture
Security Architecture (Legacy)
Topology/Dependencies
Policy/Orch (GPO, Scripts, RBA, FWP)
Instr (event, logs, DLP, ...)
Security Architecture (Virtual)
Topology/Dep. (vCenter)
Policy/Orch. (vCenter)
Instr (vCM, vCenter, DLP)
...
Security Architecture (Cloud)
SLA/Svc. Dep. (vCloud)
Policy/Orch. (vCloud Dir)
Attestation (vCM?)
Legacy
Virtual
Cloud
Analytics
Optimization
Root Cause Analysis
Proc. Correlation
Mining (new dim)
Stochastic Σ (GP)
Everything Else ∞
Discovery
Visualization
Modeling
Security Operations
Security Ops (Legacy)
Vuln Mgmt.
Incid/Event Mgmt.
Sec Config. Mgmt.
Compliance Assessment
Security Ops (Virtual)
Vuln Mgmt
Incid/Event Mgmt (event, logs_).
Sec Config Mgmt. (vCM)
Sec Config Comp Assessment (vCM)
...
Security Ops (Cloud)
Sec SLA Mgmt
Incid/Event Mgmt
Sec Deployment Mgmt.
Attestation Mgmt
Efficiency, Effectiveness, Cost

AGILITY: Continuous IMprovement



Summary

- Maintains an accurate picture of an organization's security risk posture
  - Measurements through the GRC lens. Implies common underlying semantics.
- Provides visibility into assets
  - Visibility of relationships, configuration and behavior
- Leverages automated data feeds
  - Security Content: XCCDF, OVAL, CVSS, CPE, CEE, CCE …
  - Operational Context: OVF, CIM, CMDB, SC, WS-*
- Quantifies risk – from Mission/Business objective priority to vulnerability score and coupling
- Ensures continued effectiveness of security controls – closed loop
- Informs automated or human-assisted implementation of remediation
  - Exposes operational constraints, coupling, options
- Enables prioritization of remedies – Probability, Impact (TTR), Constraints, Options, Effort (TTR)

RSA
The Security Division of EMC

Cloud Track Agenda

- 11:45 – 12:30 Security Automation for the Private Cloud:
  - Neil Ziring (Inquisitor) NSA,
  - Mischel Kwon, RSA; Steve Orrin, Intel; Jen Nowell, Symantec, Mark Ryland, Microsoft
- 13:30-14:15 Continuous Monitoring for the Cloud:
  - Kent Landfield, McAfee, Randy Barr, Qualys, Peter Mell, NIST
- 14:30-15:15 Creating Trustworthy Cloud Systems:
  - Ron Knode, CSC, Steve Orrin, Intel
- 15:45-16:30 The Need for Software Security Assurance to Secure Mission Critical Applications in the Federal Cloud:
  - RobRoy, Fortify
- 16:30-17:30 Standards to Accelerate Adoption of Cloud Computing:
  - Lee Badger and Chris Johnson, NIST