



# Risk Management in 2020 - From Continuous Monitoring to the Next Generation of Risk Scoring

**Kurt Van Etten**

Director, Product Management

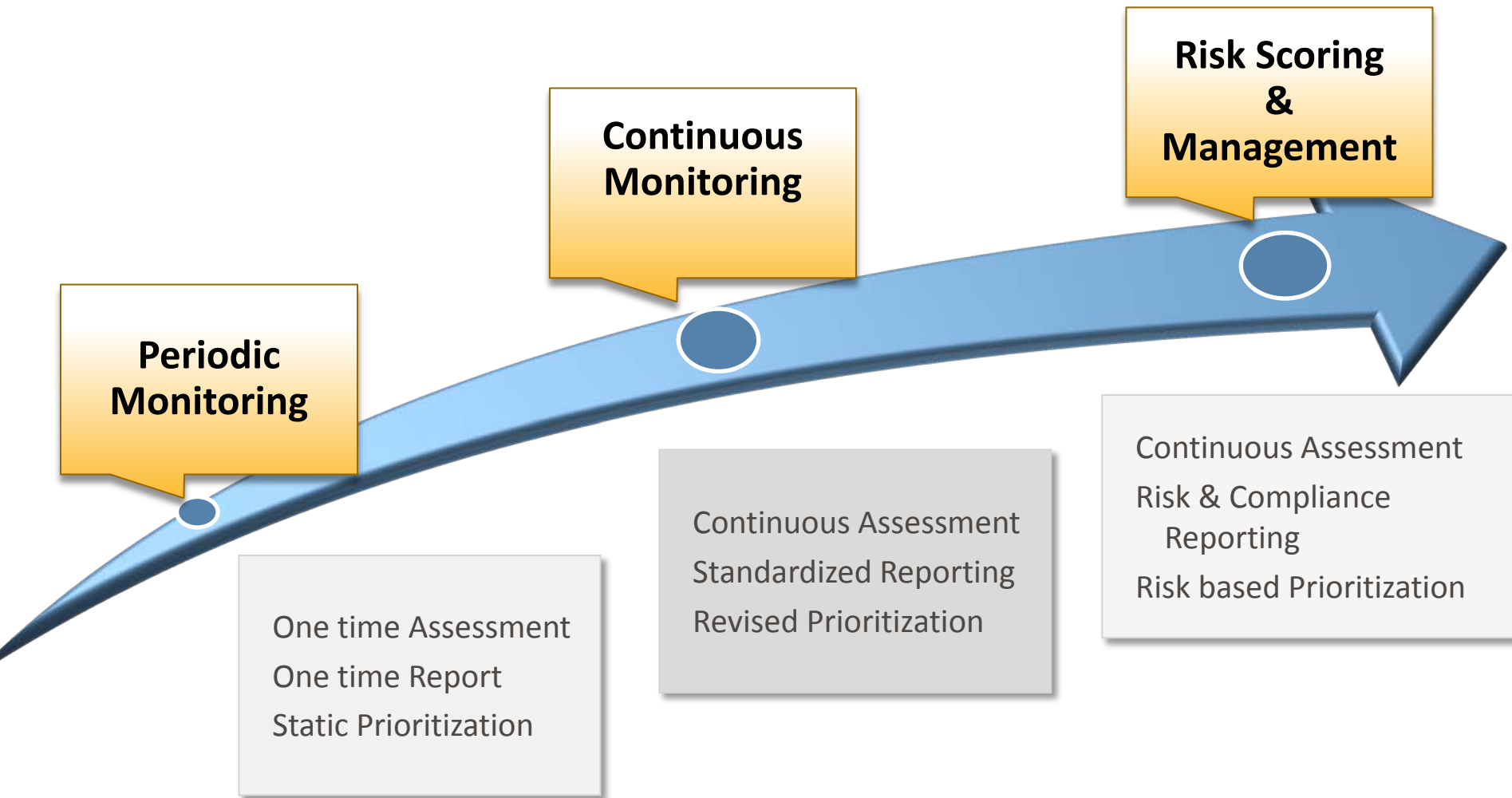
# Agenda

**1** Information Security Maturity Model

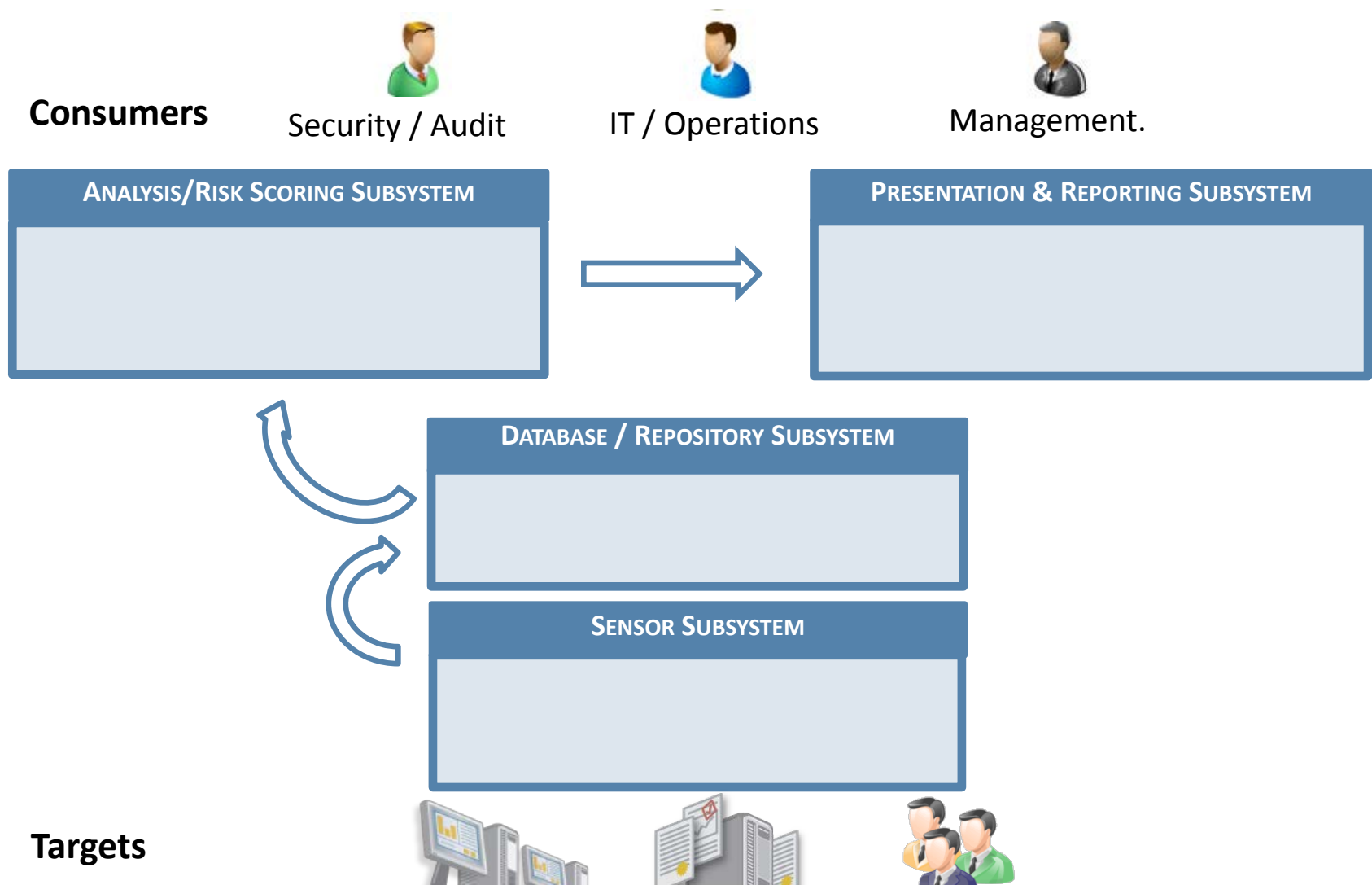
**2** Maturity Model for CEASARS framework

**3** Risk Manager

# Rapid Maturation of Information Security



# CAESARS FRAMEWORK



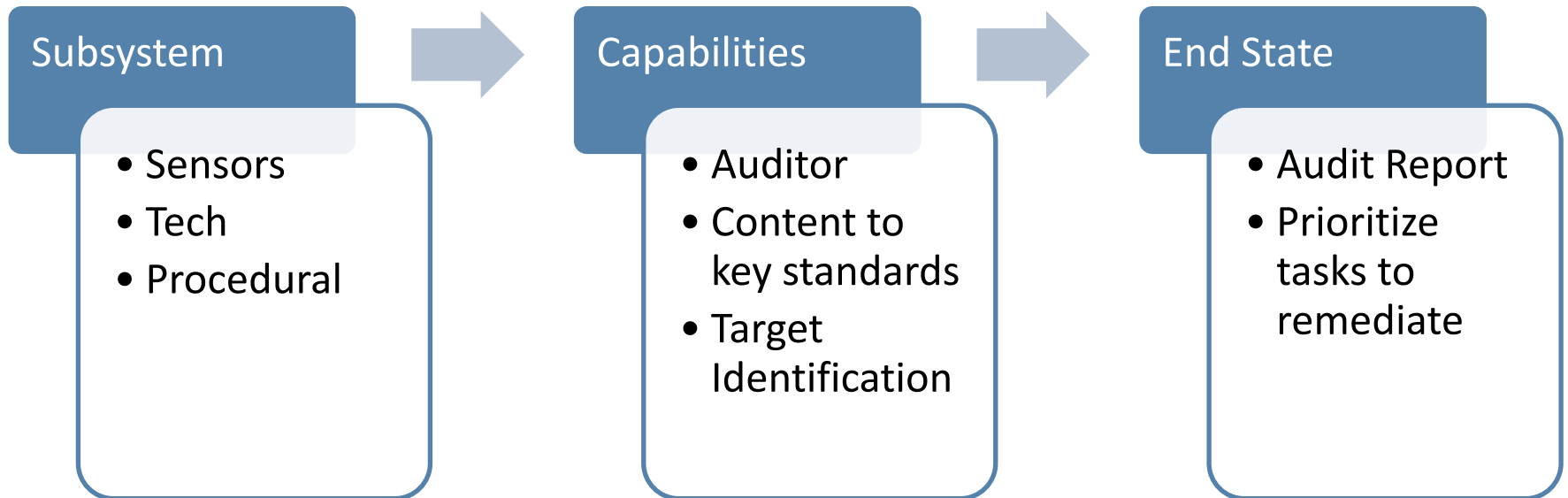
# Rapid Maturation of Information Security



**Periodic  
Monitoring**

One time Assessment  
One time Report  
Static Prioritization

# Periodic Monitoring



# Periodic Monitoring– CAESARS

Consumers



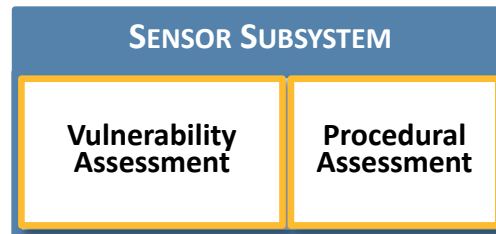
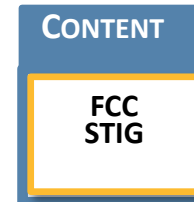
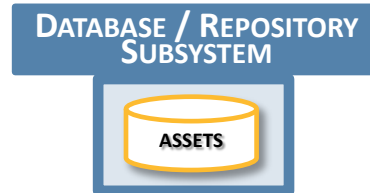
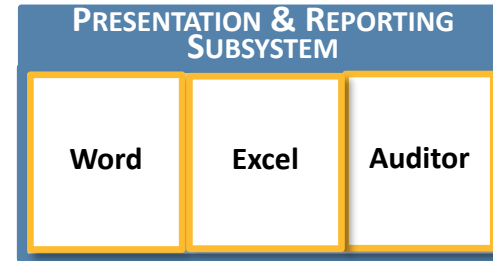
Security / Audit



IT / Operations



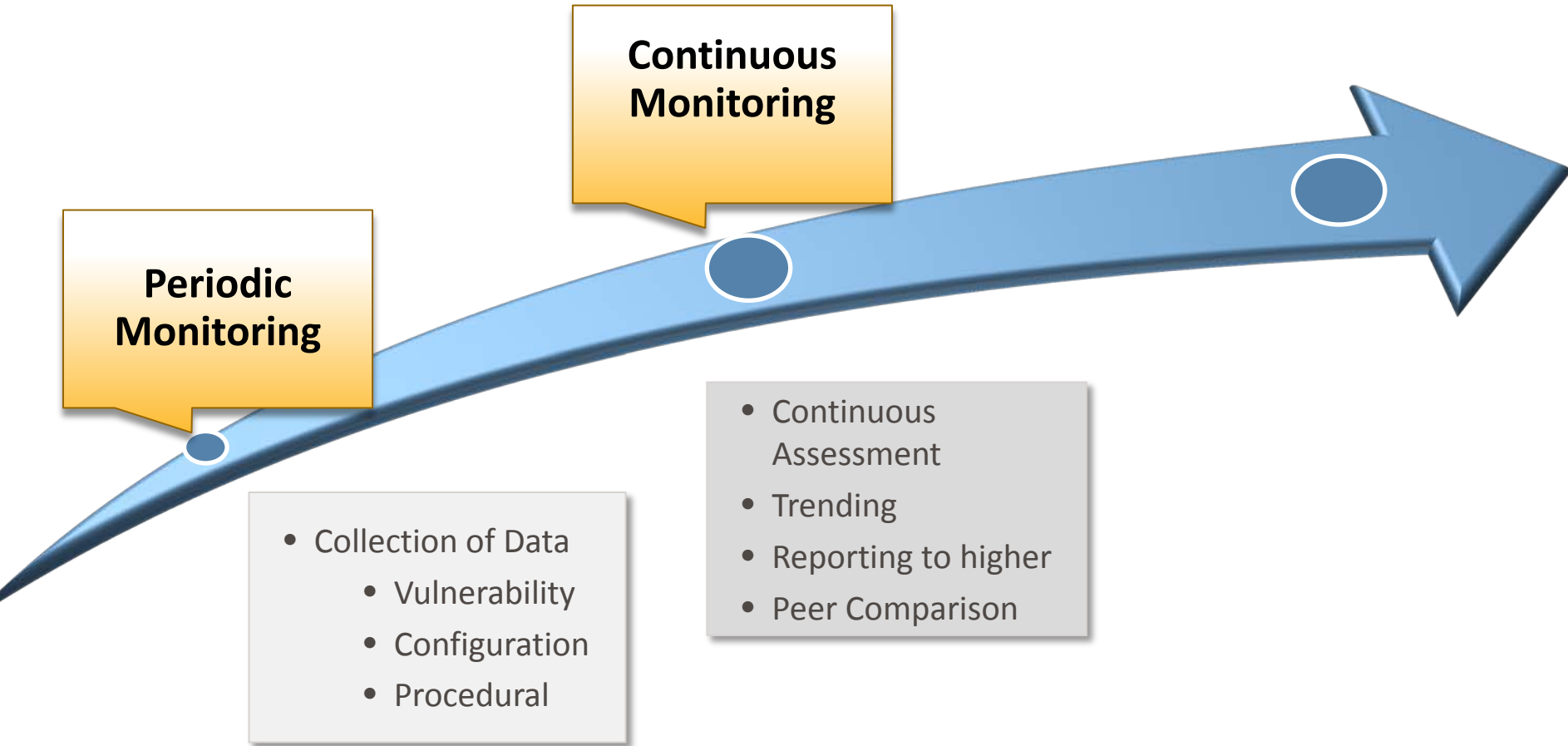
Mgmt.



Targets

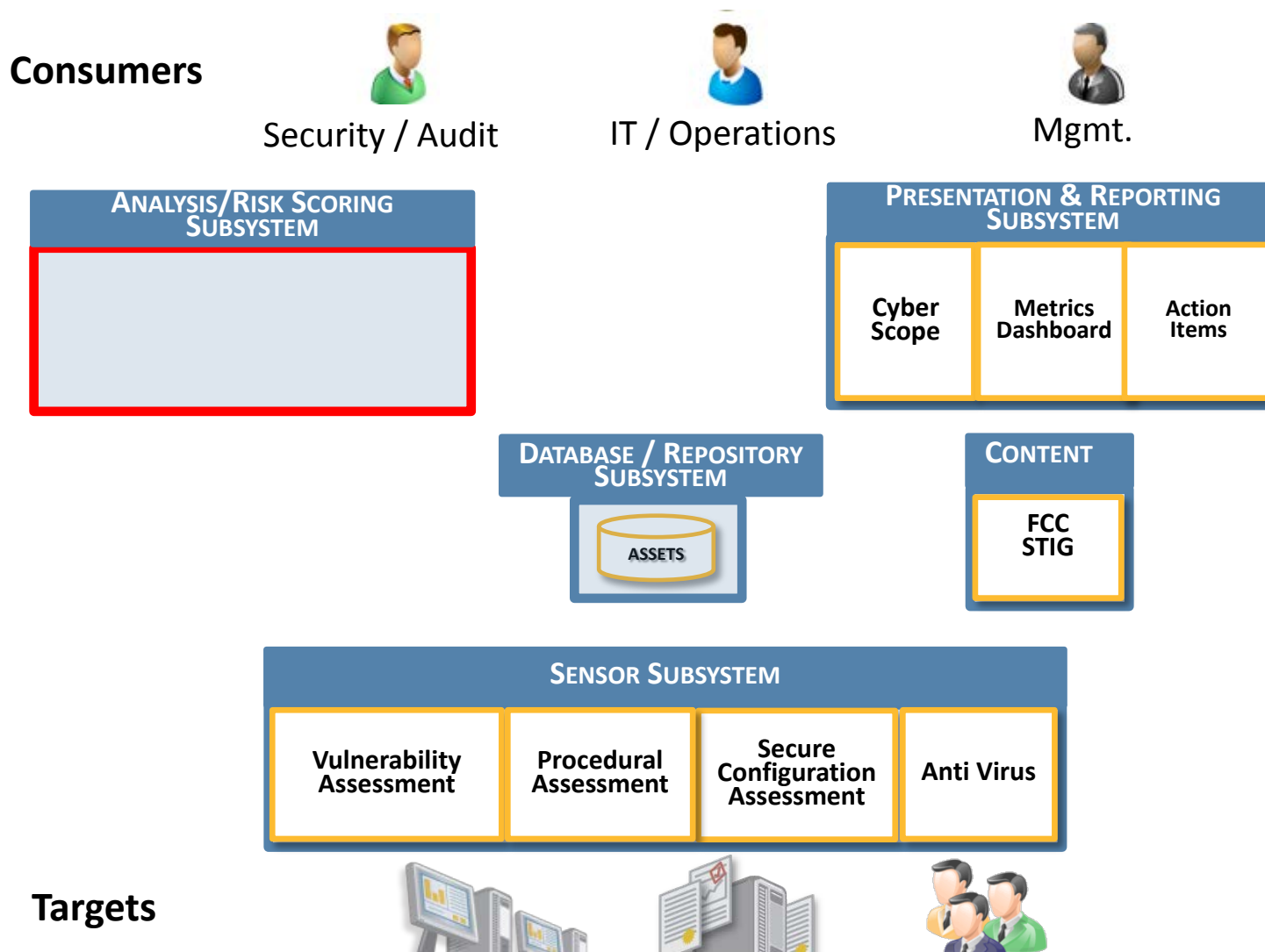


# Rapid Maturation of Information Security

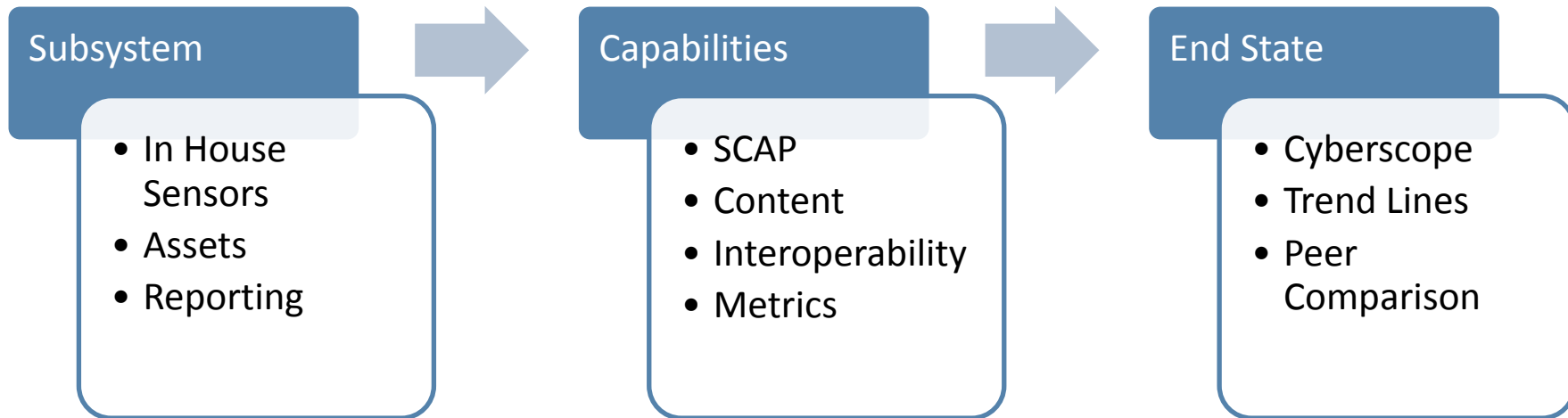




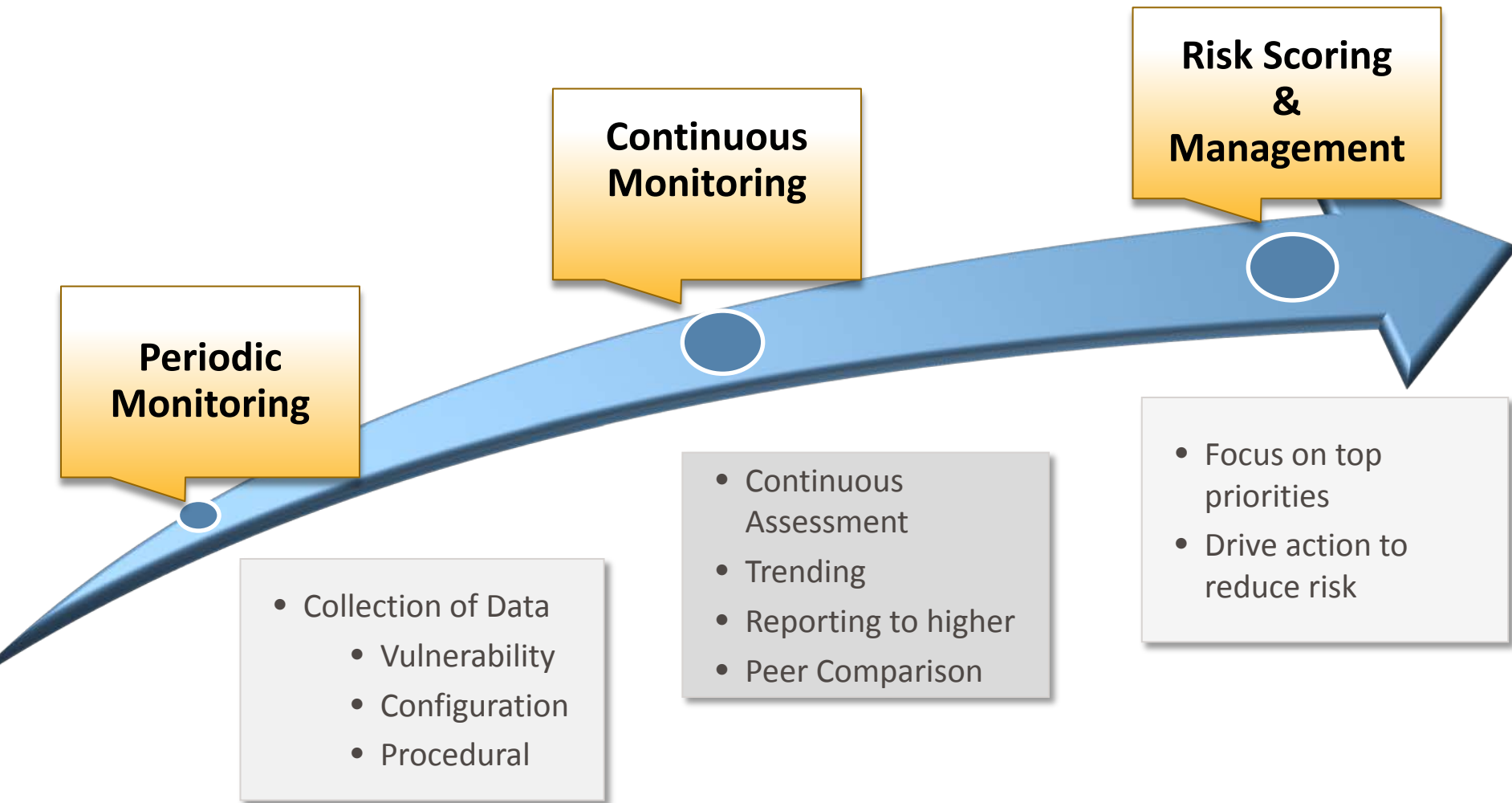
# Continuous Monitoring– CAESARS



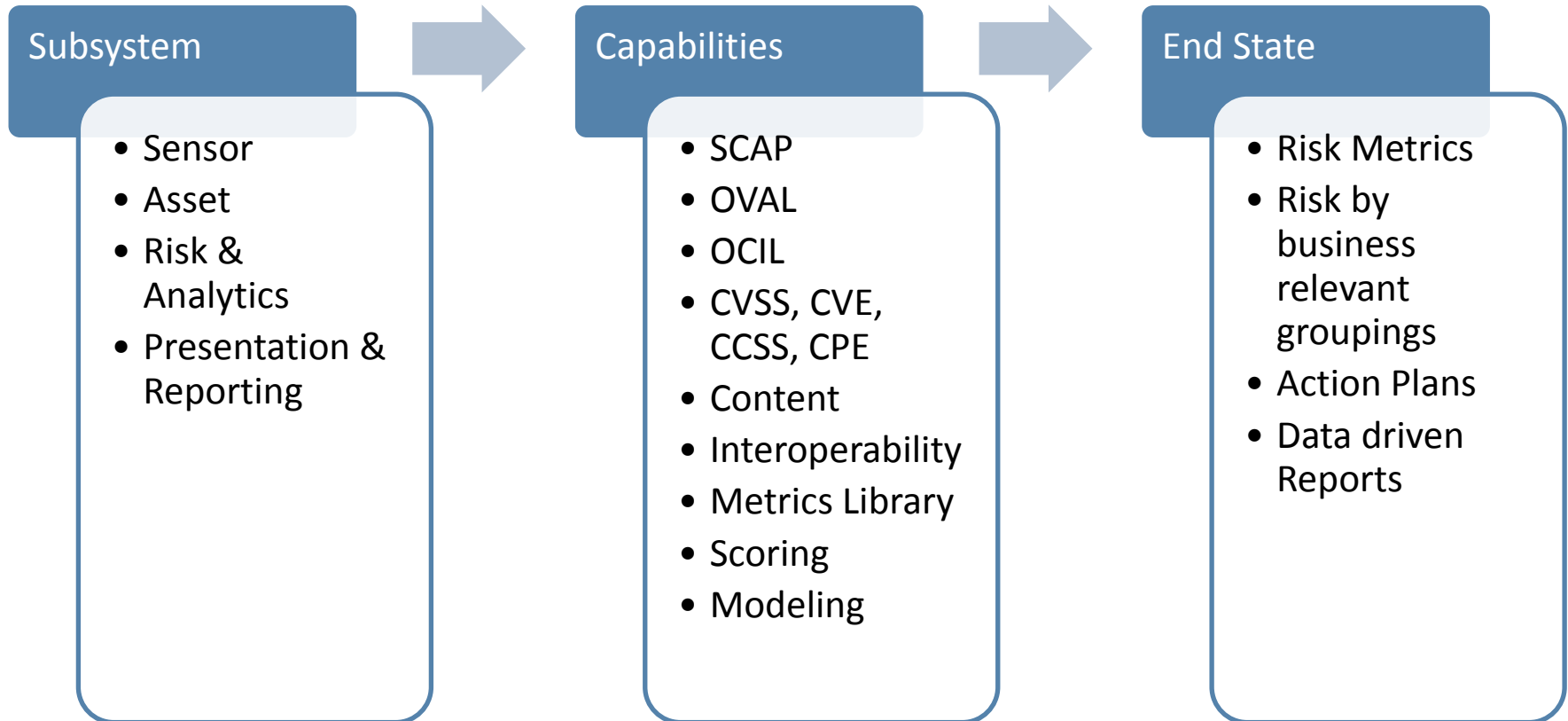
# Continuous Monitoring



# Rapid Maturation of Information Security



# Risk Management



# Risk Management– CAESARS

Consumers



Security / Audit

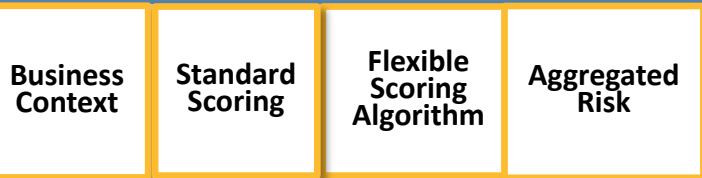


IT / Operations



Mgmt.

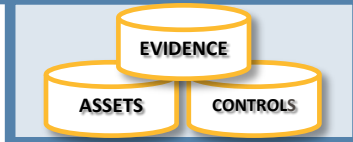
## ANALYSIS/RISK SCORING SUBSYSTEM



## PRESENTATION & REPORTING SUBSYSTEM



## DATABASE / REPOSITORY SUBSYSTEM



## CONTENT



## SENSOR SUBSYSTEM



Targets



# Risk Manager Requirements

# Symantec Control Compliance Suite – CAESARS

Consumers



Security / Audit



IT / Operations



Mgmt.

ANALYSIS/RISK SCORING SUBSYSTEM

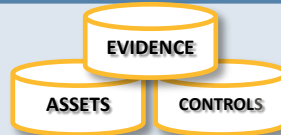
*CCS Risk Manager*

PRESENTATION & REPORTING SUBSYSTEM

CCS Reporting &  
Analytics

CCS Dynamic  
Dashboards

DATABASE / REPOSITORY  
SUBSYSTEM



CONTENT

CCS  
Content

SENSOR SUBSYSTEM

CCS  
Standards  
Manager

CCS  
Assessment  
Manager

CCS  
Virtualization  
Security  
Manager

CCS  
Vulnerability  
Manager

Extended Data  
Connectors

Targets



# CCS Connectors Roadmap

Available Now	1FQ13	2FQ13	3FQ13	Future
<b>May 2012</b>	<b>August</b>	<b>September</b>	<b>December</b>	
Courion	Aveksa	Algosec	Hytrust	Catbird Networks
Rapid7	Cenzic	Centrify	IBM - BigFix	FireMon
Salesforce.com	Core Security	Cyveillance	Onapsis	NIKSUN
VMware	eEye	Fortify (HP)	Red Seal Networks	Ping Identity
	Qualys	Hitachi ID	Tripwire	
	Sailpoint	Systems	Veracode	
	Secunia	Imperva		
	Skybox Security	Tenable		



# Risk Management Requirements

- 1) Vulnerability Management
- 2) Patch Management
- 3) Event Management
- 4) Incident Management
- 5) Malware Detection
- 6) Assct Management
- 7) Configuration Management
- 8) Network Management
- 9) License Management
- 10) Information Management
- 11) Software Assurance

**Figure 1. Continuous Monitoring Data Domains**

# Risk Management Requirements

- Extensible Configuration Checklist Description Format (XCCDF)
- Open Vulnerability and Assessment Language (OVAL)
- Open Checklist Interactive Language (OCIL)
- Common Vulnerabilities and Exposures (CVE)
- Common Configuration Enumeration (CCE)
- Common Vulnerability Scoring System (CVSS)
- Common Configuration Scoring System (CCSS)
- Common Platform Enumeration (CPE)

# Risk Manager Approach

# Symantec Approach to IT Risk Management

How do IT risks  
affect your  
mission?



How do you convey  
IT risks to your  
peers?



How do you  
drive measurable  
risk reduction?



**CCS RISK MANAGER**

**TRANSLATE**

**INFLUENCE**

**ACT**

# Introducing CCS Risk Manager

## CCS RISK MANAGER

### TRANSLATE

- » Define virtual business assets
- » Connect related IT assets
- » Create business view of IT risk

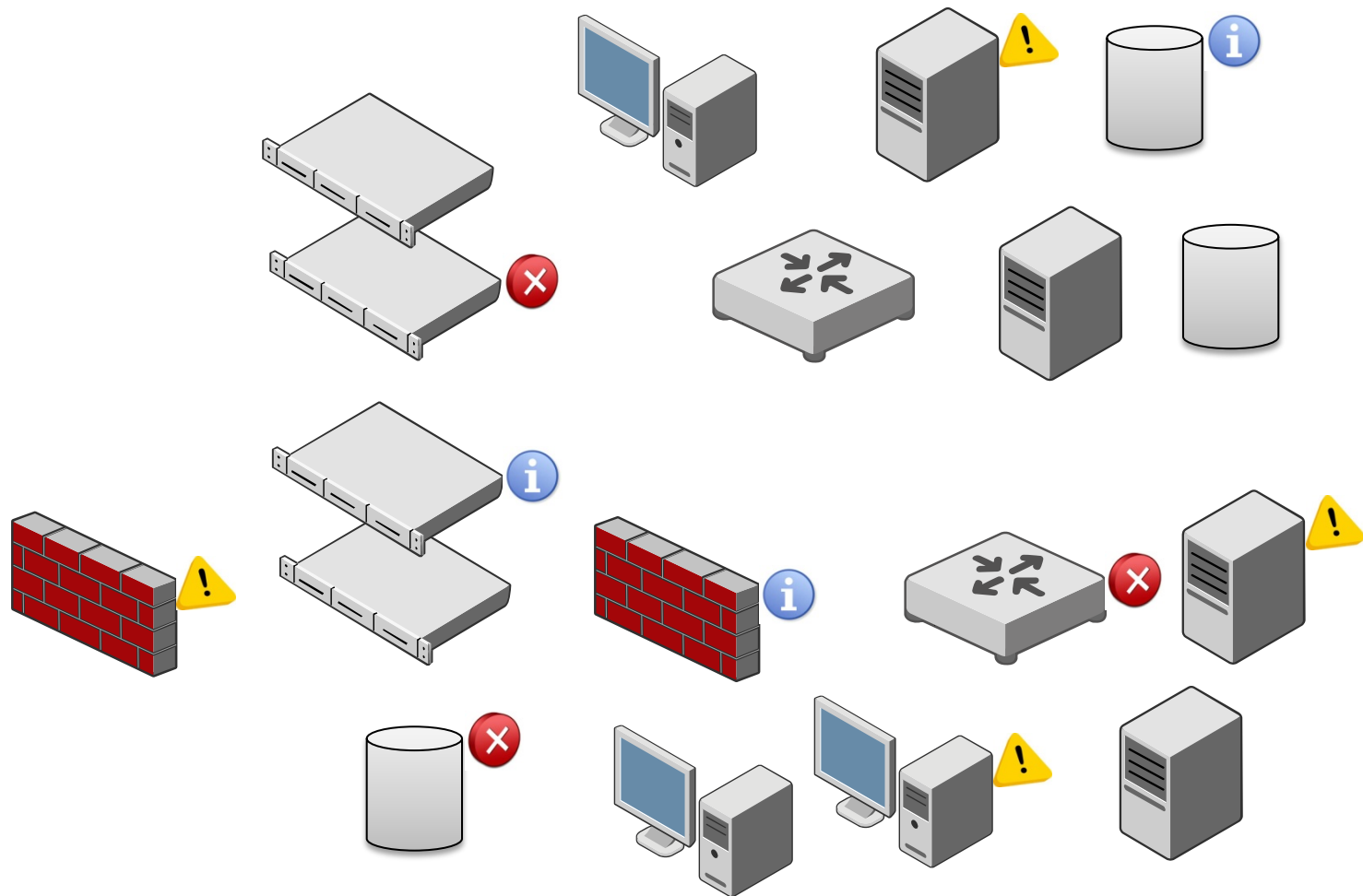
### INFLUENCE

- » Convey IT risk in business terms
- » Customized views for greater impact
- » Justify new security investments

### ACT

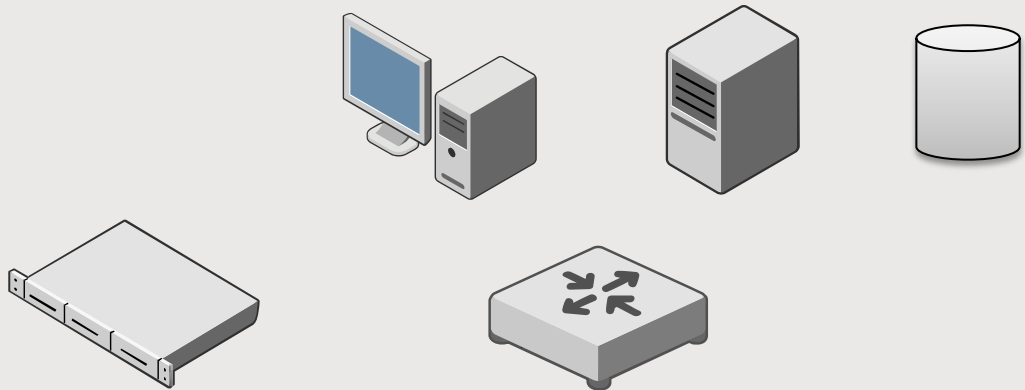
- » Prioritize based on business impact
- » Align Security and IT Operations
- » Track risk reduction over time

# Current View of IT Risk – Technology Centric

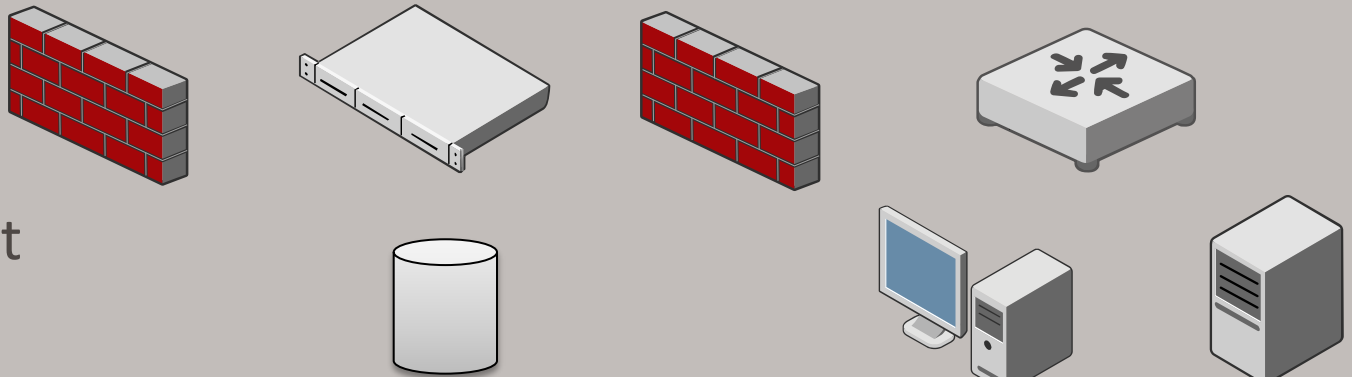


# Translating IT Risk

Transaction Processing System

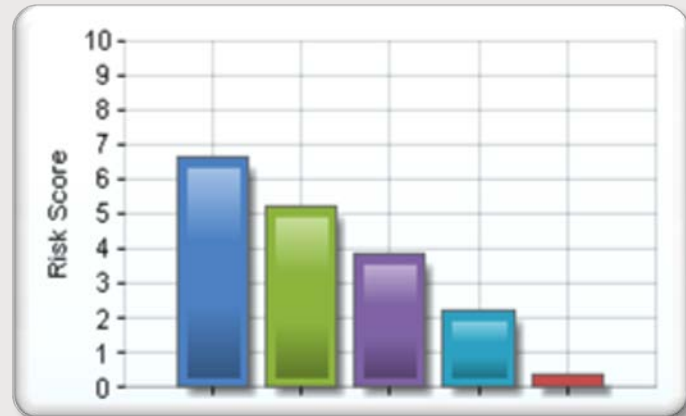


Case Management



# Translating IT Risk

Transaction Processing System



Case Management





# Using Risk to Drive Accountability and Action

Transaction Processing System



Plan Name	Risk Objective	Status	Current Score	Projected Score	Target Date	Owner
Plan B	Secure Configuration	Submitted	3.65	2.75	3/15/12	Bob
Plan C	Patch Level Standard	Submitted	4.22	1.81	4/11/12	Joe
Plan A	Info Sec Standard	Completed	2.23	2.23	1/10/12	Joe
Plan D	Protect Web Servers	Submitted	3.51	2.10	2/28/12	Dave

# CCS Risk Manager Highlights



**Define** a business asset you want to manage



**Visualize** and understand IT risk for this business asset



**Prioritize** remediation based on IT risk, not technical severity



**Monitor** risk reduction over time

# Visualize and Understand IT Risk

## Enterprise Wide View of Business Risk



# Visualize and Understand IT Risk

## Balanced View of Business and Operational Metrics



# Prioritize Remediation Based on Risk

## Risk Modeling

Symantec Control Compliance Suite

Dashboards Questionnaires Policy Risk Management Downloads Settings

Risk Modeling Remediation Plans

Print

### Analyze Risk

#### Protect Internet Banking Web Servers

##### Risk Objective Details

Risk Objective : [Protect Internet Banking Web Servers](#)

Owner : CCSAPPS\Jeff

Drag a column header here to group by that column

Action	Asset Name	Risk	Current Risk Score	Projected Risk Score	Category	Asset Type	Asset Path	History
None	CCSAPPS\SCAP-XPSP2	Critical Vulnerabilities Assessment	3.6	3.6	Security and Risk Asse	Windows Machine	Asset System\People's	
None	CCSAPPS\W2K8ENT-IBM	Critical Vulnerabilities Assessment	6.1	6.1	Security and Risk Asse	Windows Machine	Asset System\People's	
None	CCSAPPS\SCAP-XPSP2	Secure System Configuration - Access Control	2.5	2.5	Configuration Managen	Windows Machine	Asset System\People's	
None	CCSAPPS\W2K8ENT-IBM	Secure System Configuration - Access Control	2.5	2.5	Configuration Managen	Windows Machine	Asset System\People's	
None	CCSAPPS\LAB5-209-170	Secure System Configuration - Access Control	4.03	0	Configuration Managen	Windows Machine	Asset System\XYZ Bar	
None	CCSAPPS\SCAP-XPSP2	Secure System Configuration - Configuration M	3.21	3.21	Configuration Managen	Windows Machine	Asset System\People's	
None	CCSAPPS\W2K8ENT-IBM	Secure System Configuration - Configuration M	4.41	0	Configuration Managen	Windows Machine	Asset System\People's	
None	CCSAPPS\LAB5-209-170	Secure System Configuration - Configuration M	2.81	2.81	Configuration Managen	Windows Machine	Asset System\XYZ Bar	

1 of 1

Current Risk Score: 3.64      Projected Risk Score: 2.75

Create Plan Cancel

# Prioritize Remediation Based on Risk

## Remediation Plan by Risk Objective

Create Plan

### Protect Internet Banking Web Servers

Plan Name:\*

Description:

Assigned To:

Complete By:

Recommended Action:

Risk Objective: Protect Internet Banking Web Servers  
Asset Group: N/A  
Initiated By: CCSAPPS\Jeff  
Current Risk Score: 3.64  
Projected Residual Risk Score: 2.75

### Risks for Remediation

Risks for Acceptance

Control Statement	Asset	Current Risk	Assigned To	Recommended Action	Include Remediation Steps
<a href="#">Secure System Configuration - Access Control</a>	CCSAPPS\LAB5-209-170	4.03	Jeff Rohan	Change Access rights	<input checked="" type="checkbox"/>
<a href="#">Secure System Configuration - Configuration Management</a>	CCSAPPS\W2K8ENT-IBM	4.41	Jeff Rohan	change configurations settings	<input checked="" type="checkbox"/>

Submit Via:

Review & finalize remediation plan

Replan Save Next



# Monitor Risk Reduction Over Time

## Manage Remediation Plans

The screenshot displays the Symantec Control Compliance Suite Risk Management interface. At the top, there is a navigation bar with icons for Dashboards, Questionnaires, Policy, Risk Management, Downloads, and Settings. Below this, a green notification bar states: "Remediation Plan saved and Email notification sent successfully." The main content area is titled "Remediation Plans" and includes a table with the following columns: Action, Plan Name, Risk Objective, Status, Current Risk Score, Projected Risk Score, Complete By, and Assigned To. The first row of the table is highlighted with a red border.

Action	Plan Name	Risk Objective	Status	Current Risk Score	Projected Risk Score	Complete By	Assigned To
	Internet Banking Web Servers - Action 2	Protect Internet Banking Web Servers	Submitted	3.65	2.75	30-11-2011	Jeff Rohan
	Internet Banking Web Servers Remediation Plan	Protect Internet Banking Web Servers	Submitted	3.65	1.81	30-04-2012	Jeff Rohan
	80% remediation target	Overall Risk Assessment	Completed	2.57	1.53	30-11-2011	Jeff Rohan
	Secure Configurations Plan	Overall Risk Assessment	Submitted	2.57	2.23	30-11-2011	Jeff Rohan
	Remediate Mobile Device Configurations	Overall Risk Assessment	Completed	2.57	2.10	30-11-2011	Steve Marcus
	Mobile Devices Fix Plan	Conformance to the Information security standards	Completed	2.51	2.02	06-11-2011	Jeff Rohan
	Secure Configurations Plan 1	Conformance to the Information security standards	Submitted	2.51	2.25	30-11-2011	Jeff Rohan
	Accepted Risks Plan	Conformance to the Information security standards	Submitted	2.51	2.21	09-12-2011	Jeff Rohan

Track risk reduction for remediation plans

# Effective Risk Management

1

## Data Driven View of Risk

- Cross-reference multiple data points for a true view of risk
- Combine 3<sup>rd</sup> party data for 'composite' risk score
- Easily digest and distill data from thousands of devices

2

## Ability to Show Business Value

- Map IT assets to business assets
- Present relevant information to business peers
- Flexible reporting – avoid costly re-mapping efforts

3

## Move Beyond Risk Assessment to Risk Monitoring & Management

- Track objectives and monitor risk over time
- Develop action plans to manage entire remediation process
- Demonstrate risk reduction over time





# Thank you!

**Copyright © 2010 Symantec Corporation. All rights reserved.** Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.

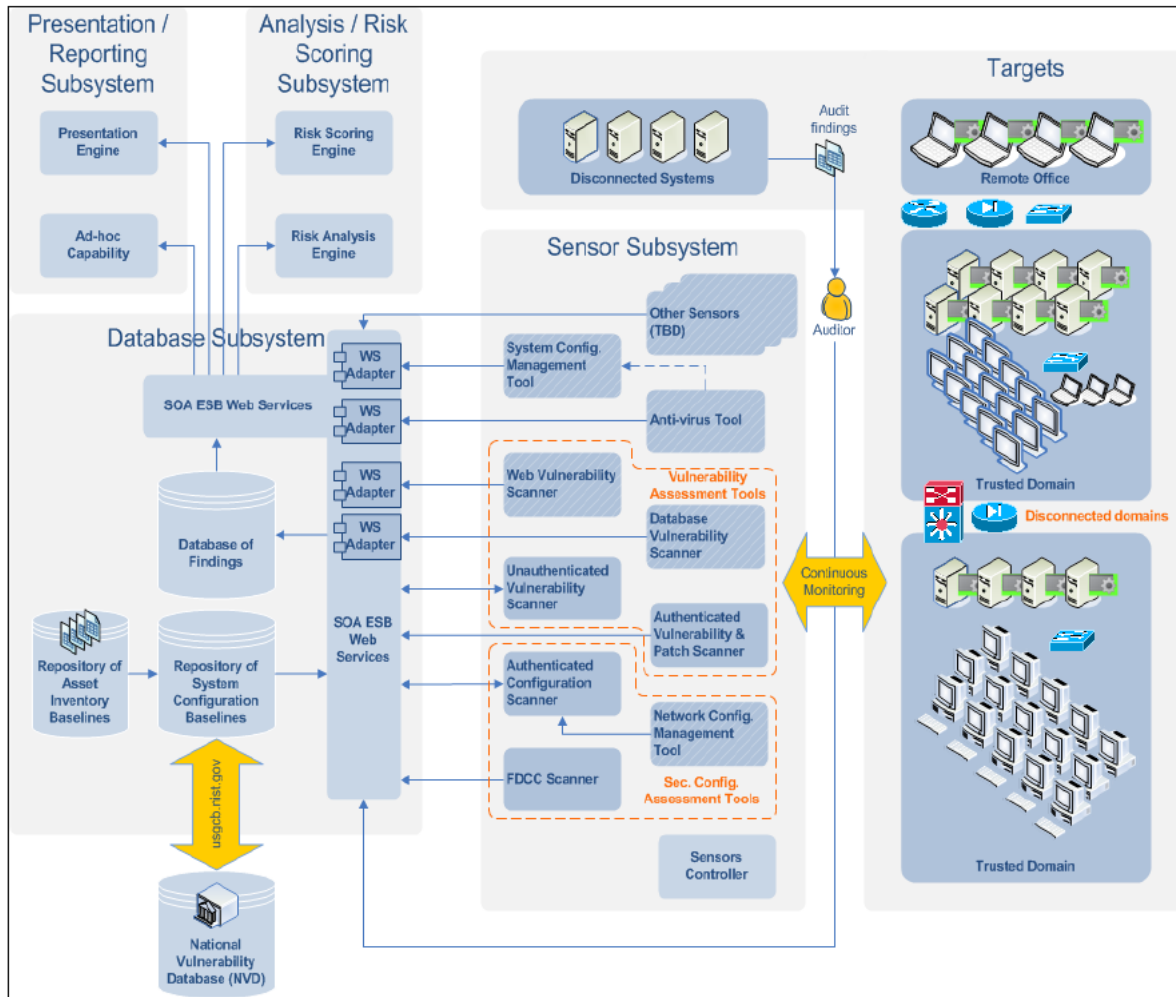


Figure 3. Contextual Description of the CAESARS System

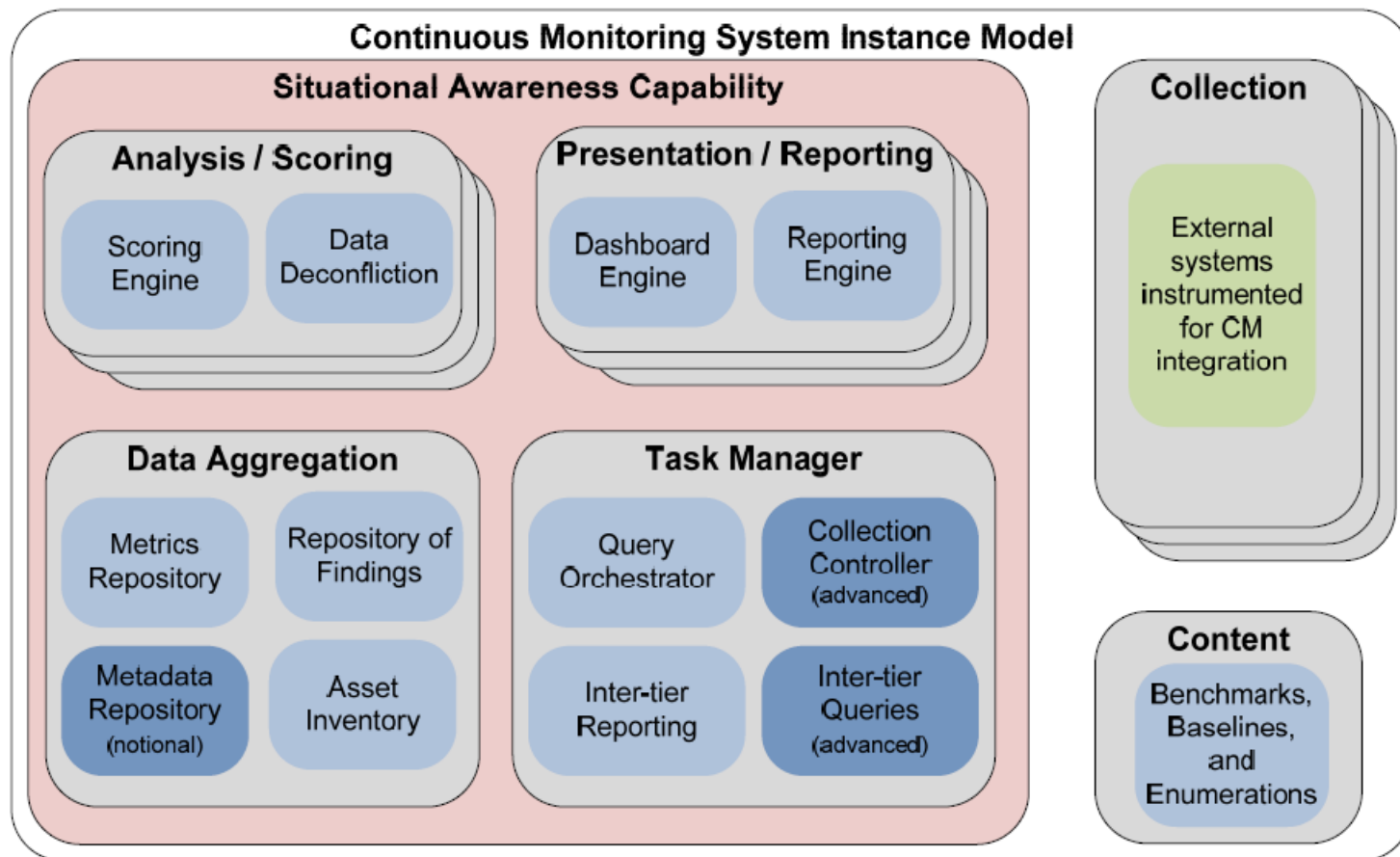
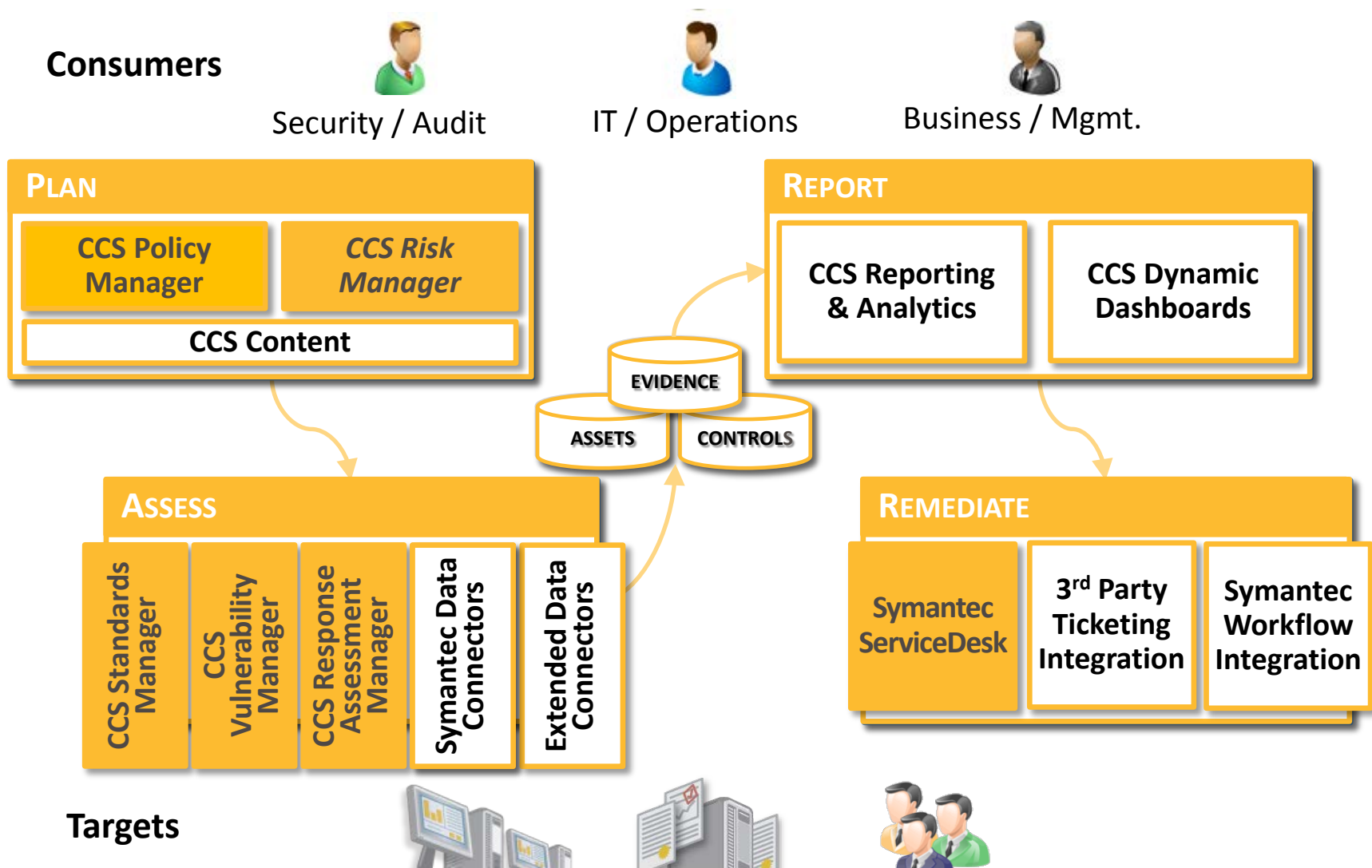


Figure 4. CAESARS Framework Extension Subsystems

# Symantec Control Compliance Suite – Overview



# Symantec Control Compliance Suite – Interoperability

## SCAP

SCAP 1.0 Windows fully supported in Standards Manager

Future: SCAP 1.2 CCS Support in Q2 CY13

## OCIL

OCIL for Assessment Manager will be supported in Q4 CY12.

## CYBER SCOPE REPORTING

CCS Cyber scope Reporting Q4 CY12.