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

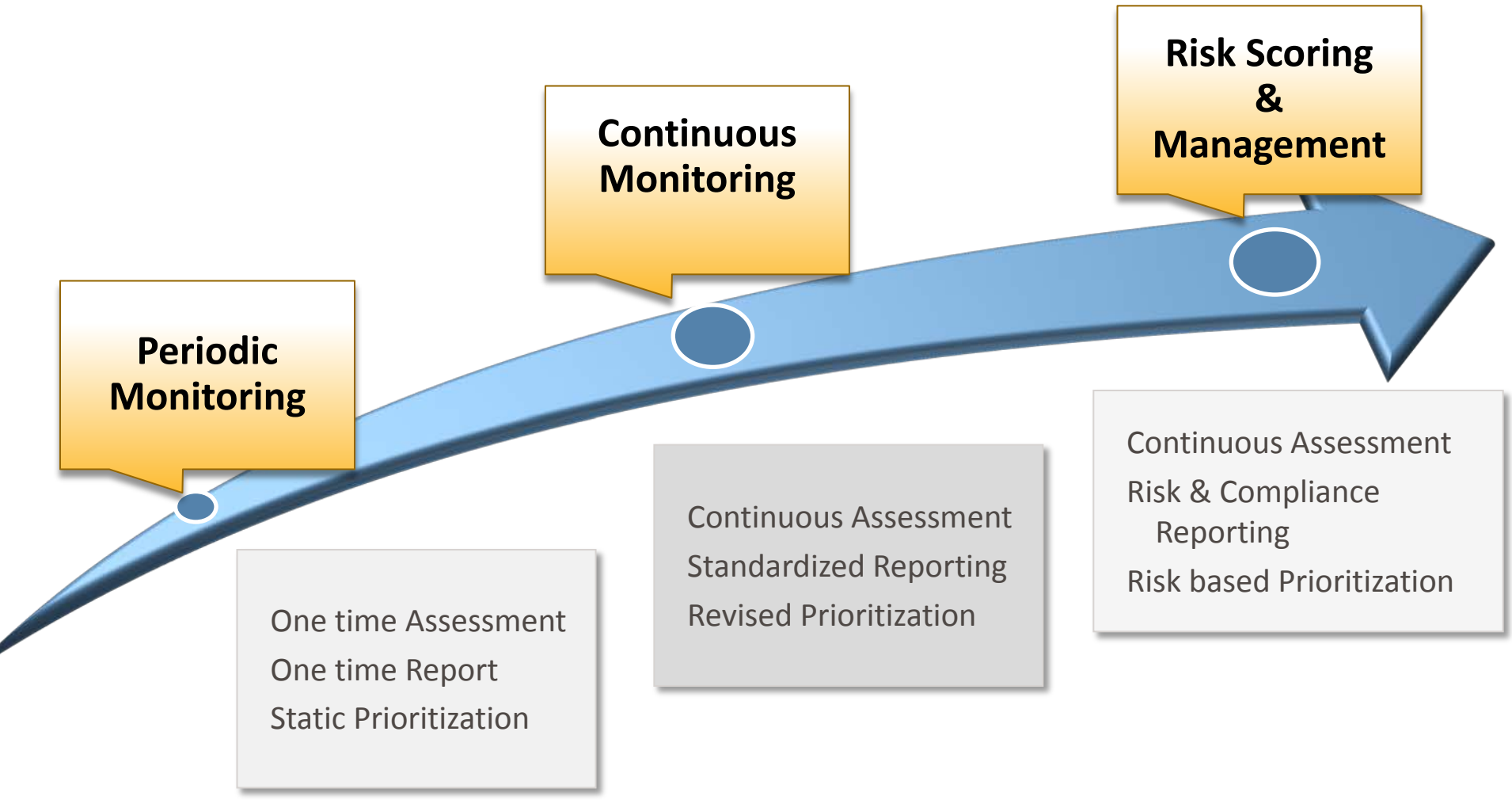
Kurt Van Etten

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

Consumers

Security / Audit

IT / Operations

Management.

ANALYSIS/RISK SCORING SUBSYSTEM

PRESENTATION & REPORTING SUBSYSTEM

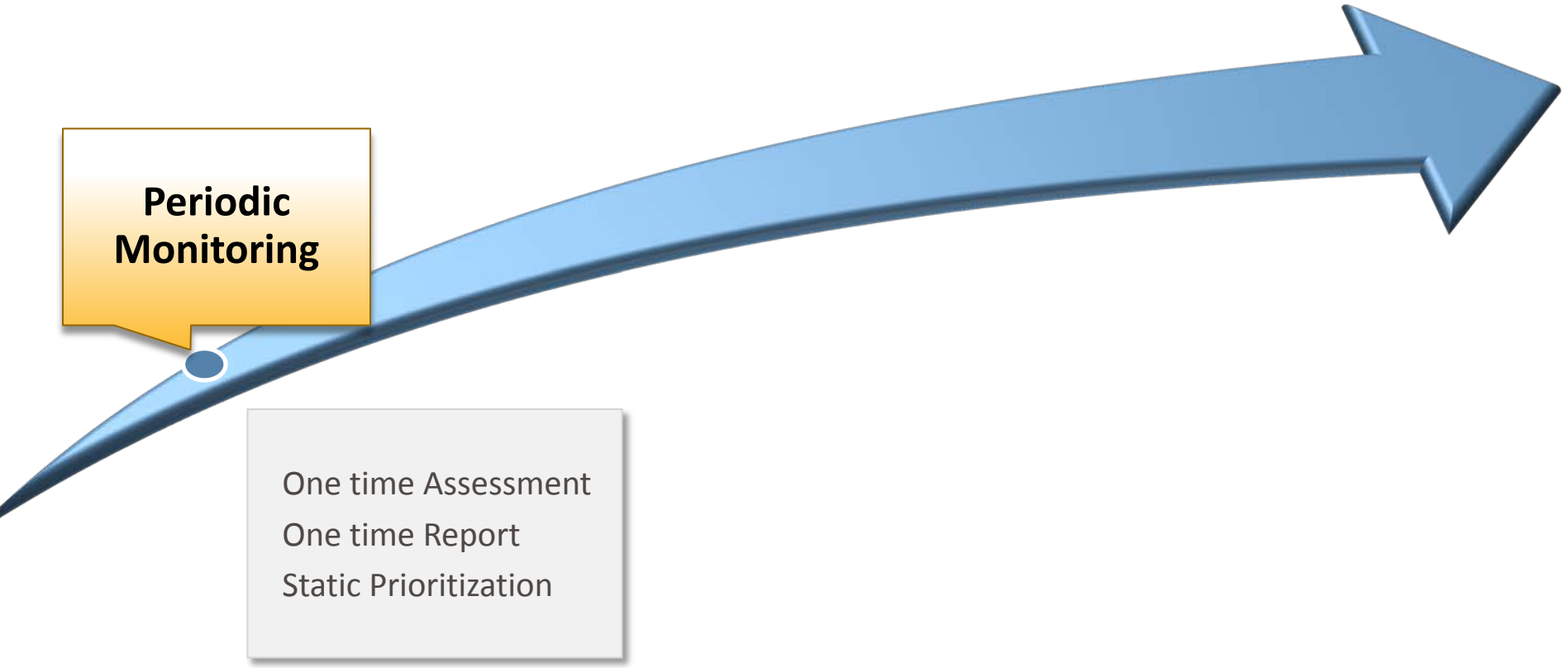
DATABASE / REPOSITORY SUBSYSTEM

SENSOR SUBSYSTEM

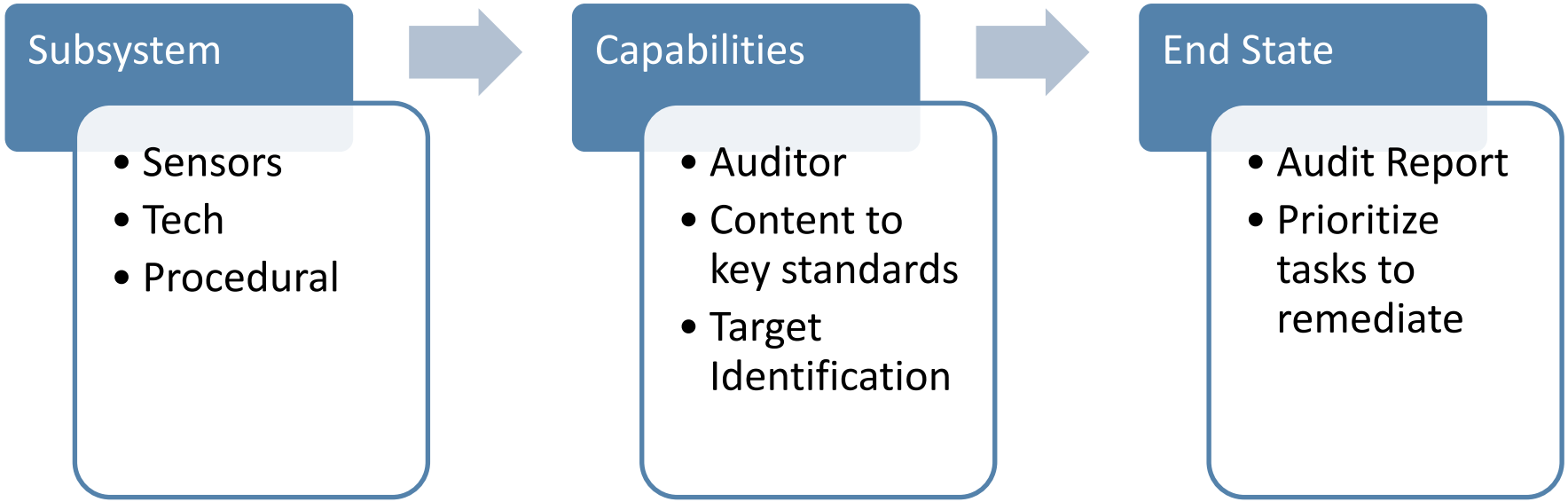
Targets

** Planned new product. Roadmap subject to change.*

Rapid Maturation of Information Security



Periodic Monitoring



Periodic Monitoring– CAESARS

Consumers

Security / Audit

IT / Operations

Mgmt.

ANALYSIS/RISK SCORING SUBSYSTEM

PRESENTATION & REPORTING SUBSYSTEM

Word | Excel | Auditor

DATABASE / REPOSITORY SUBSYSTEM

ASSETS

CONTENT

FCC STIG

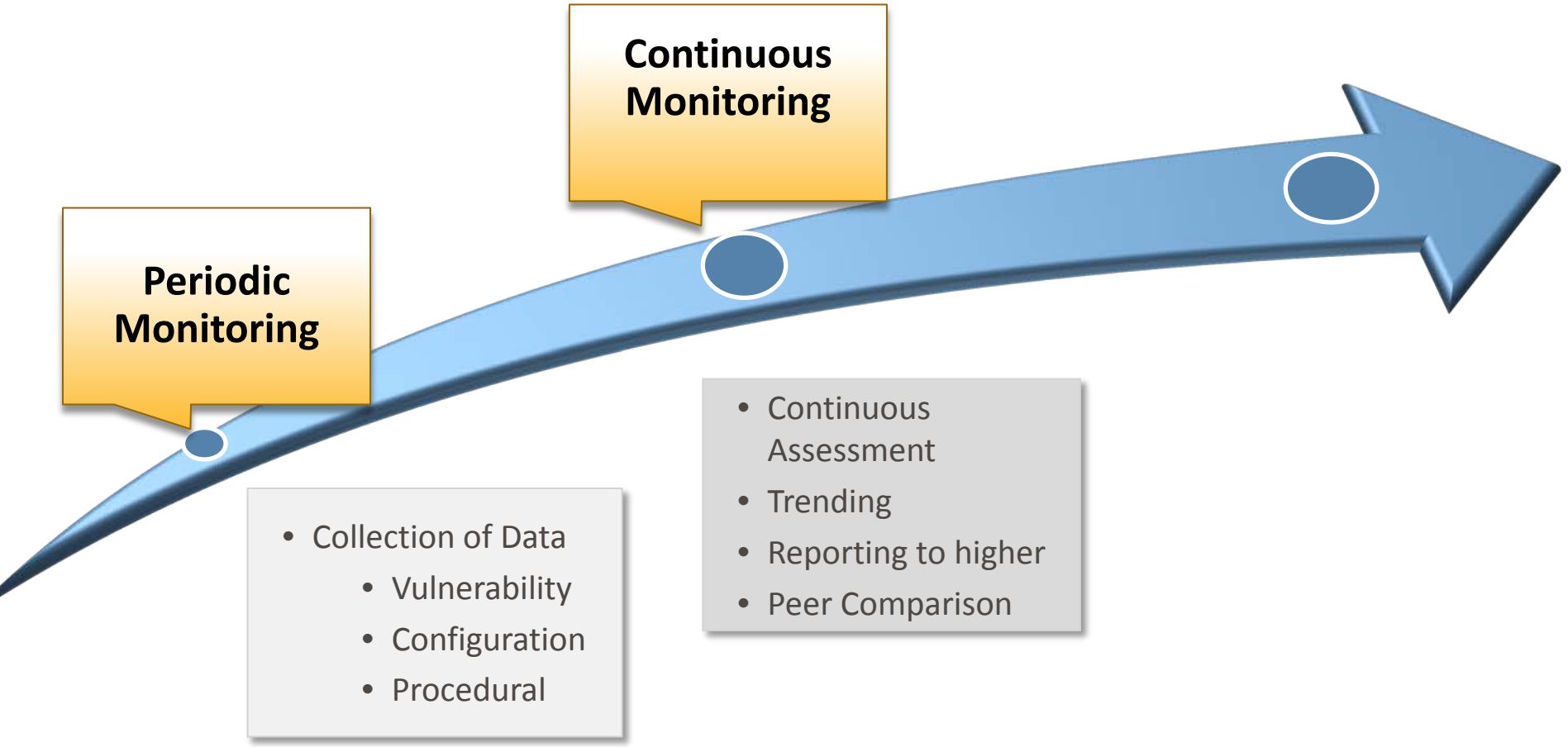
SENSOR SUBSYSTEM

Vulnerability Assessment | Procedural Assessment

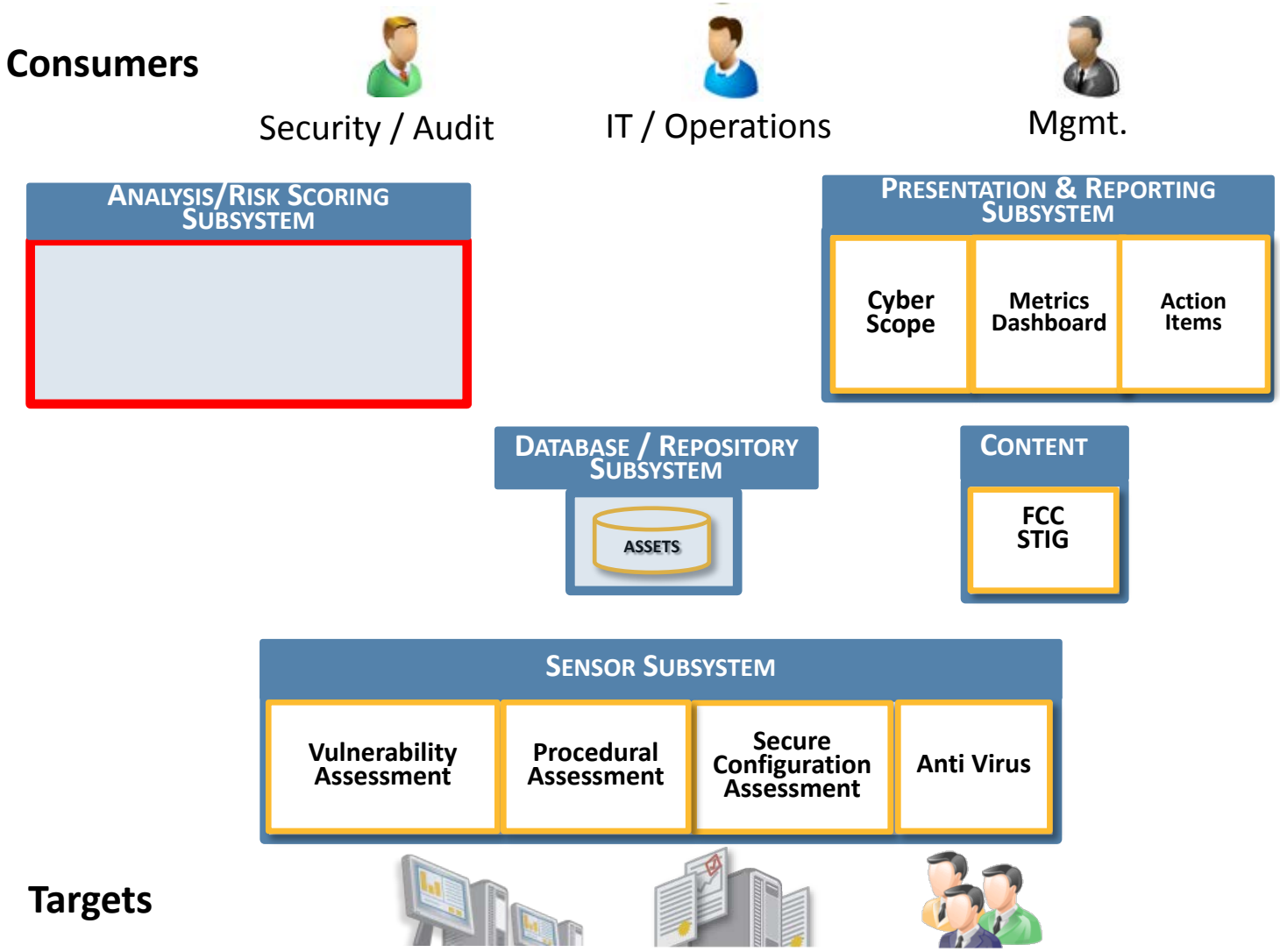
Targets

** Planned new product. Roadmap subject to change.*

Rapid Maturation of Information Security

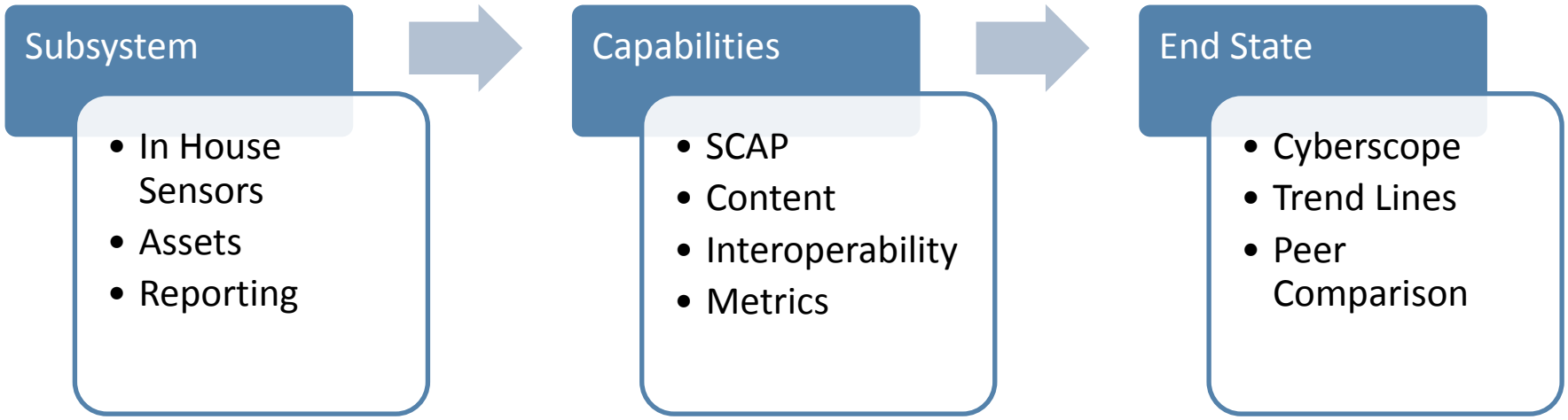


Continuous Monitoring– CAESARS

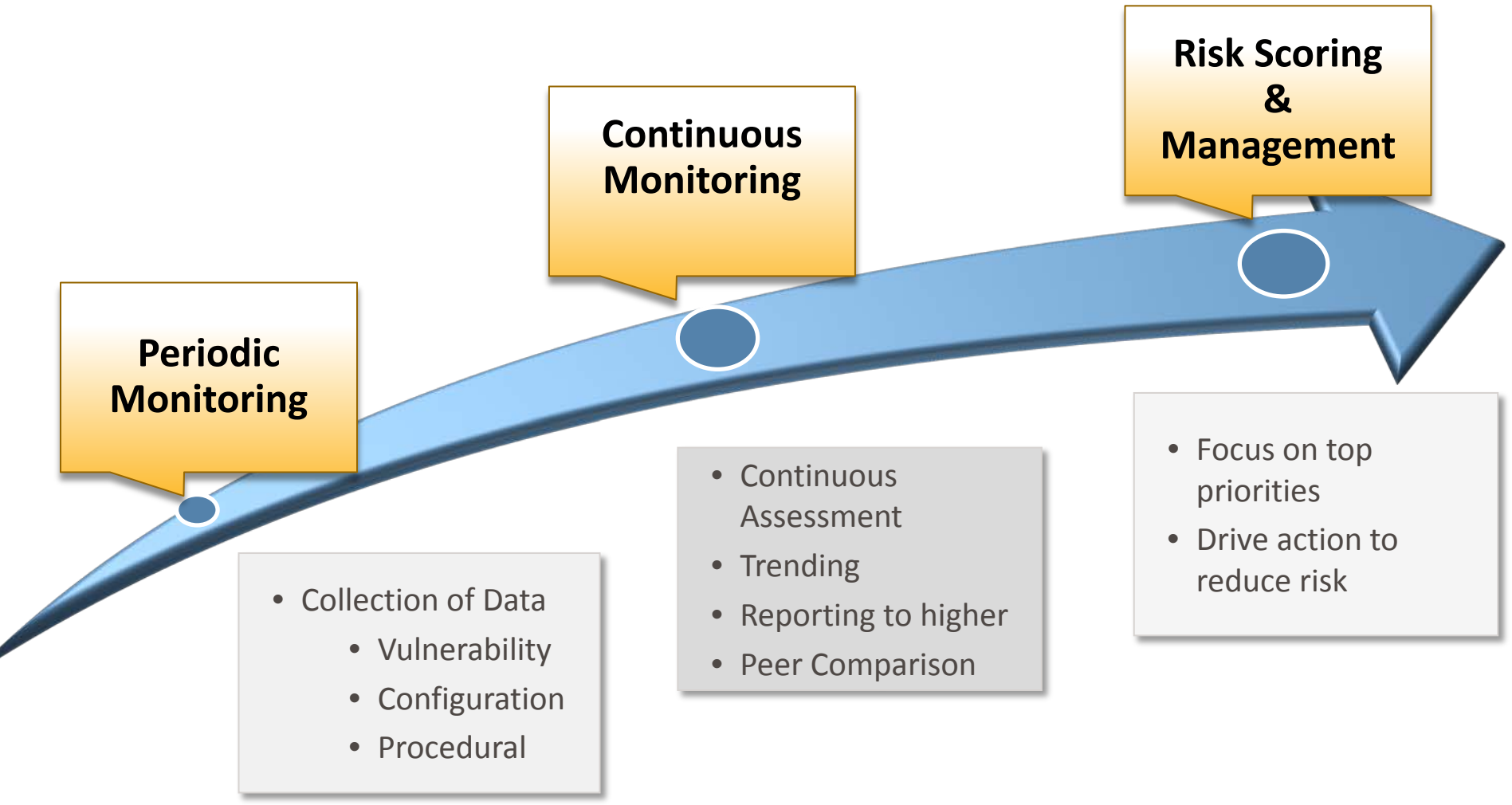


** Planned new product. Roadmap subject to change.*

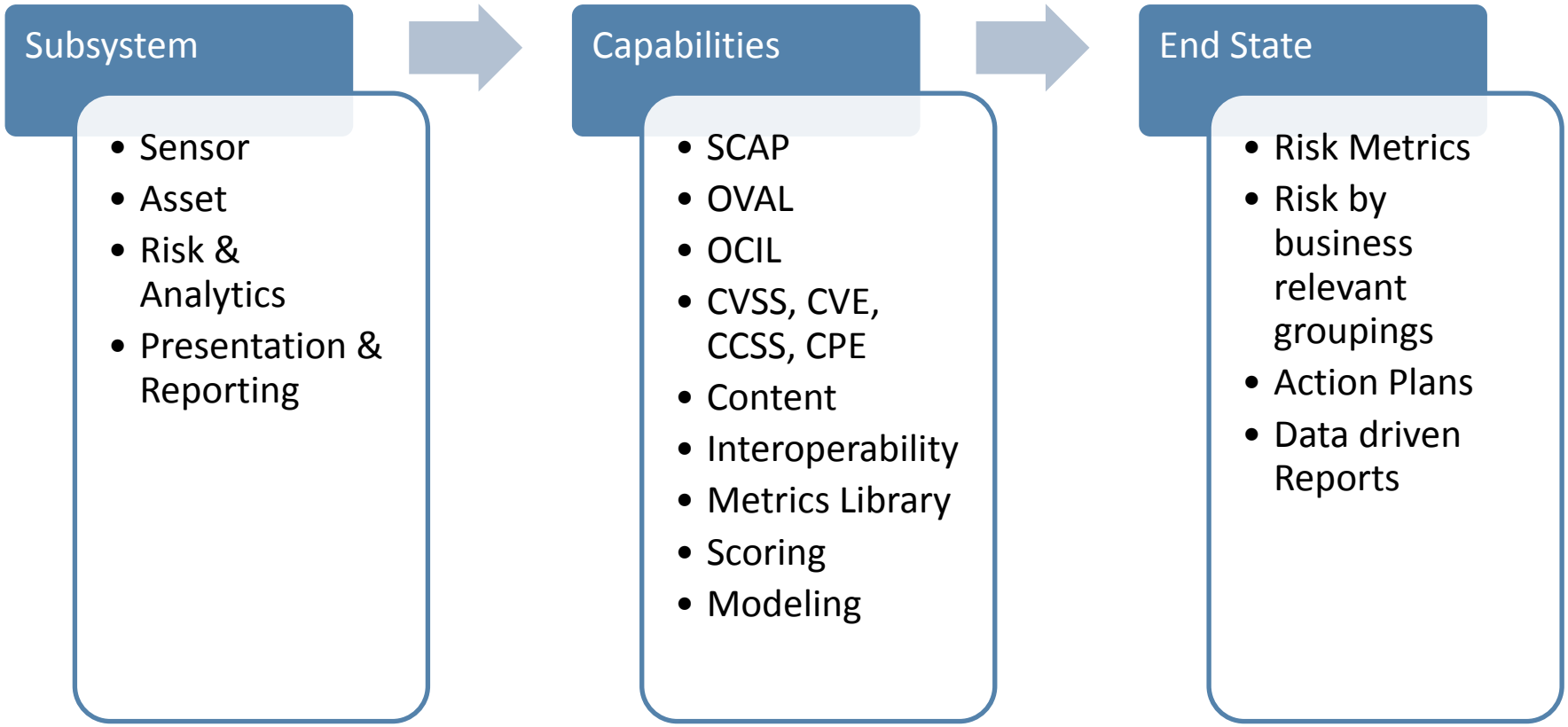
Continuous Monitoring



Rapid Maturation of Information Security



Risk Management



Risk Management– CAESARS

Consumers

Security / Audit

IT / Operations

Mgmt.

ANALYSIS/RISK SCORING SUBSYSTEM

- Business Context
- Standard Scoring
- Flexible Scoring Algorithm
- Aggregated Risk

PRESENTATION & REPORTING SUBSYSTEM

- Cyber Scope
- Mandate Based Reporting
- User Specific Dashboards
- Drill Down Dashboards

DATABASE / REPOSITORY SUBSYSTEM

CONTENT

- FCC STIG

SENSOR SUBSYSTEM

- Vulnerability Assessment
- Procedural Assessment
- Secure Configuration Assessment
- Anti Virus
- Data Loss Prevention
- Etc…

Targets

** Planned new product. Roadmap subject to change.*

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

** Planned new product. Roadmap subject to change.*

CCS Connectors Roadmap

Available Now	1FQ13	2FQ13	3FQ13	Future
May 2012	**August**	**September**	**December**	
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

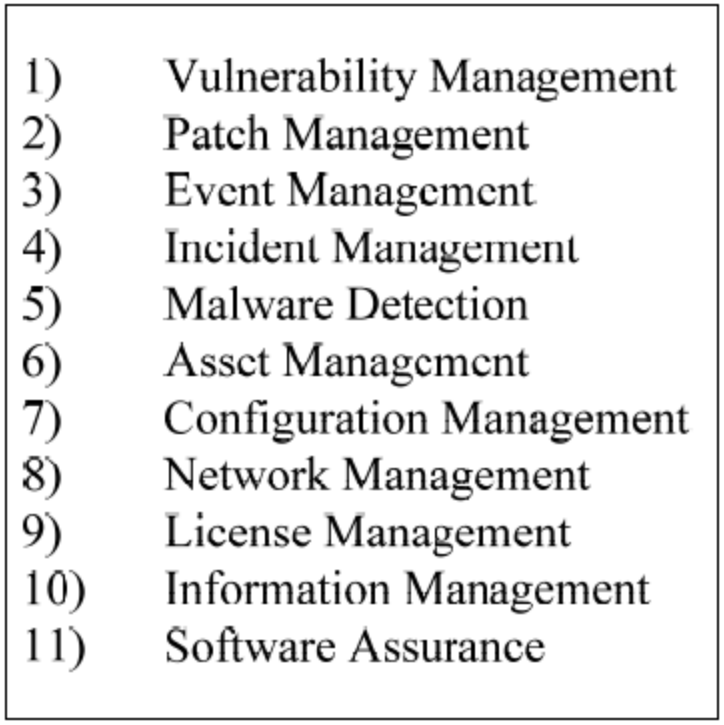


Figure 1. Continuous Monitoring Data Domains

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?

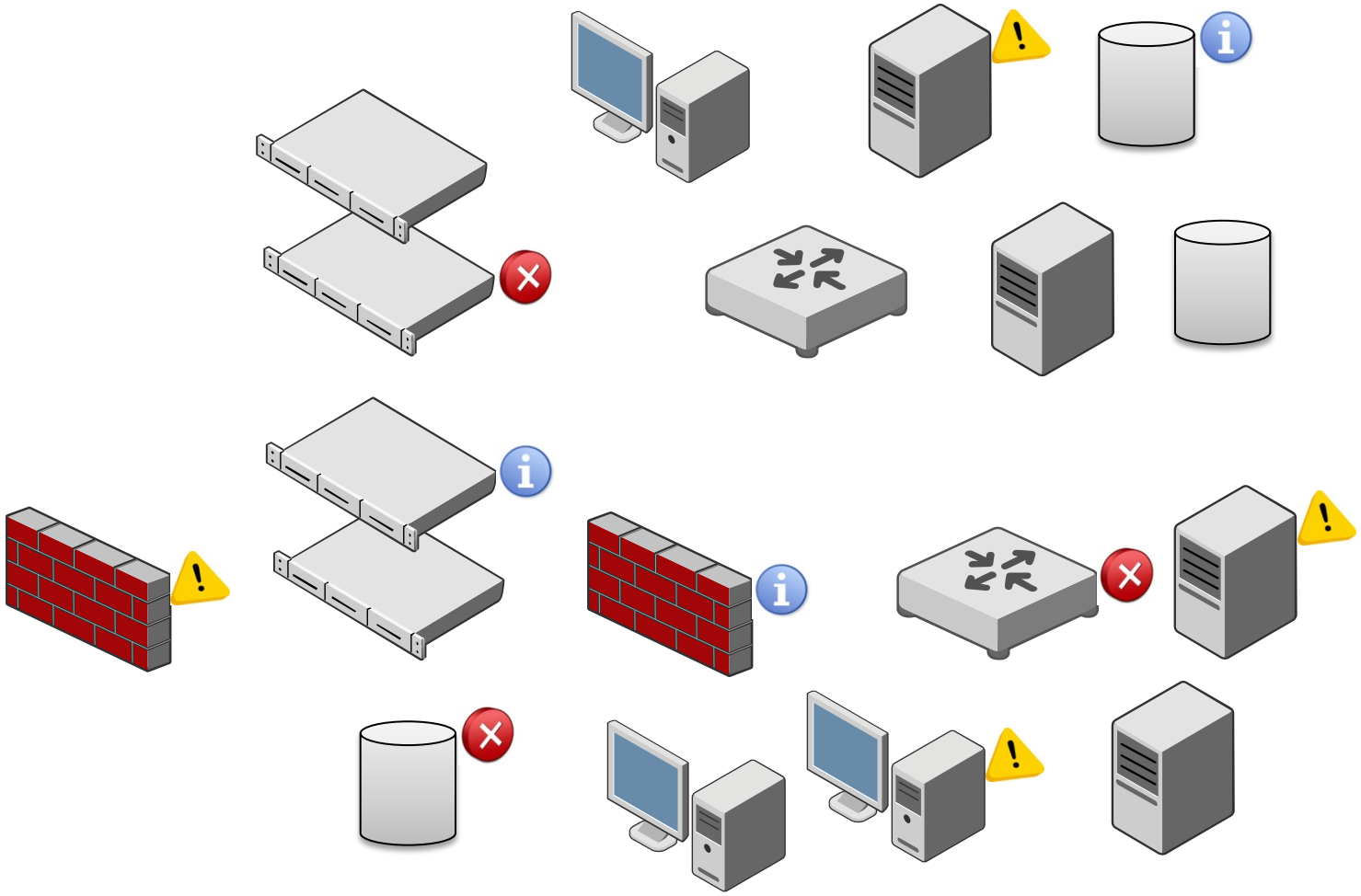
How do you drive measurable risk reduction?

Introducing CCS Risk Manager

CCS RISK MANAGER

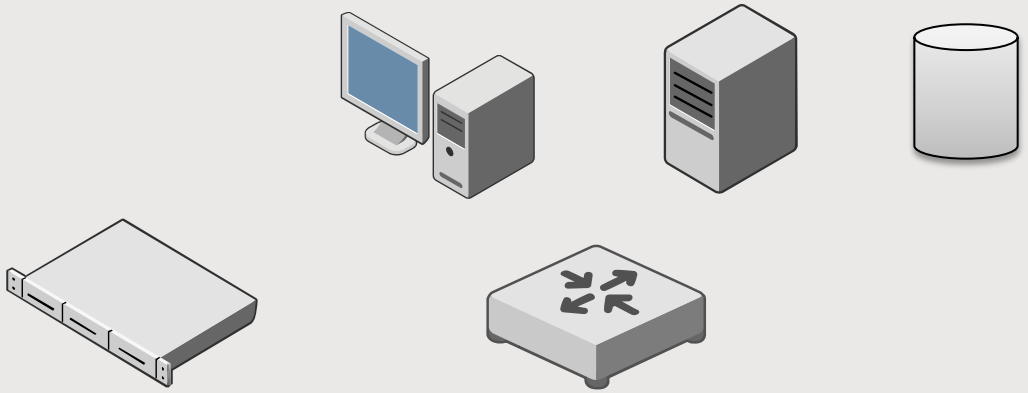
TRANSLATE	INFLUENCE	ACT
» Define virtual business assets	» Convey IT risk in business terms	» Prioritize based on business impact
» Connect related IT assets	» Customized views for greater impact	» Align Security and IT Operations
» Create business view of IT risk	» Justify new security investments	» Track risk reduction over time

Current View of IT Risk – Technology Centric

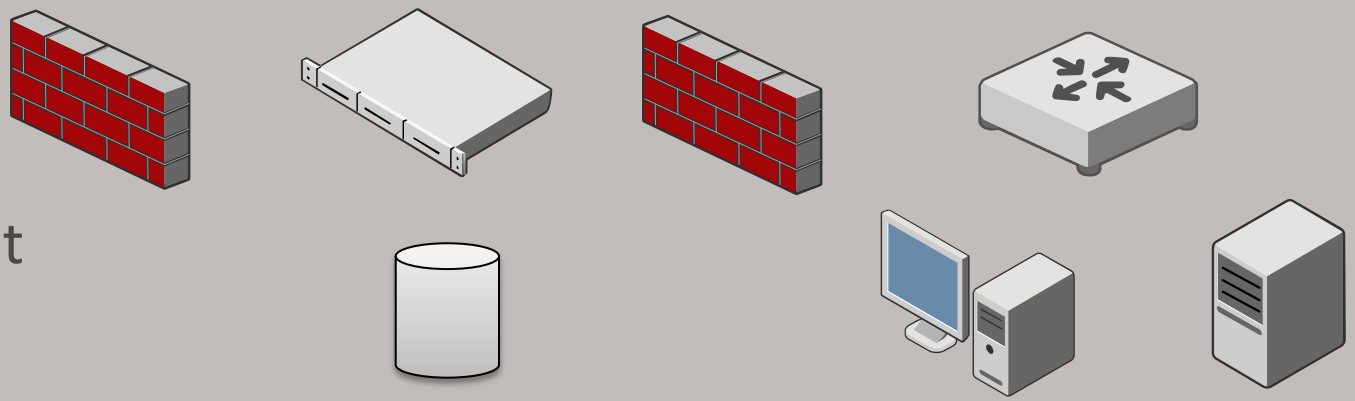


Translating IT Risk

Transaction Processing System

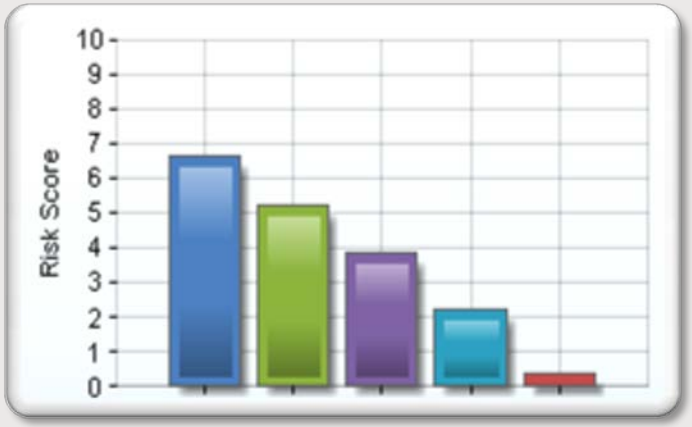


Case Management



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

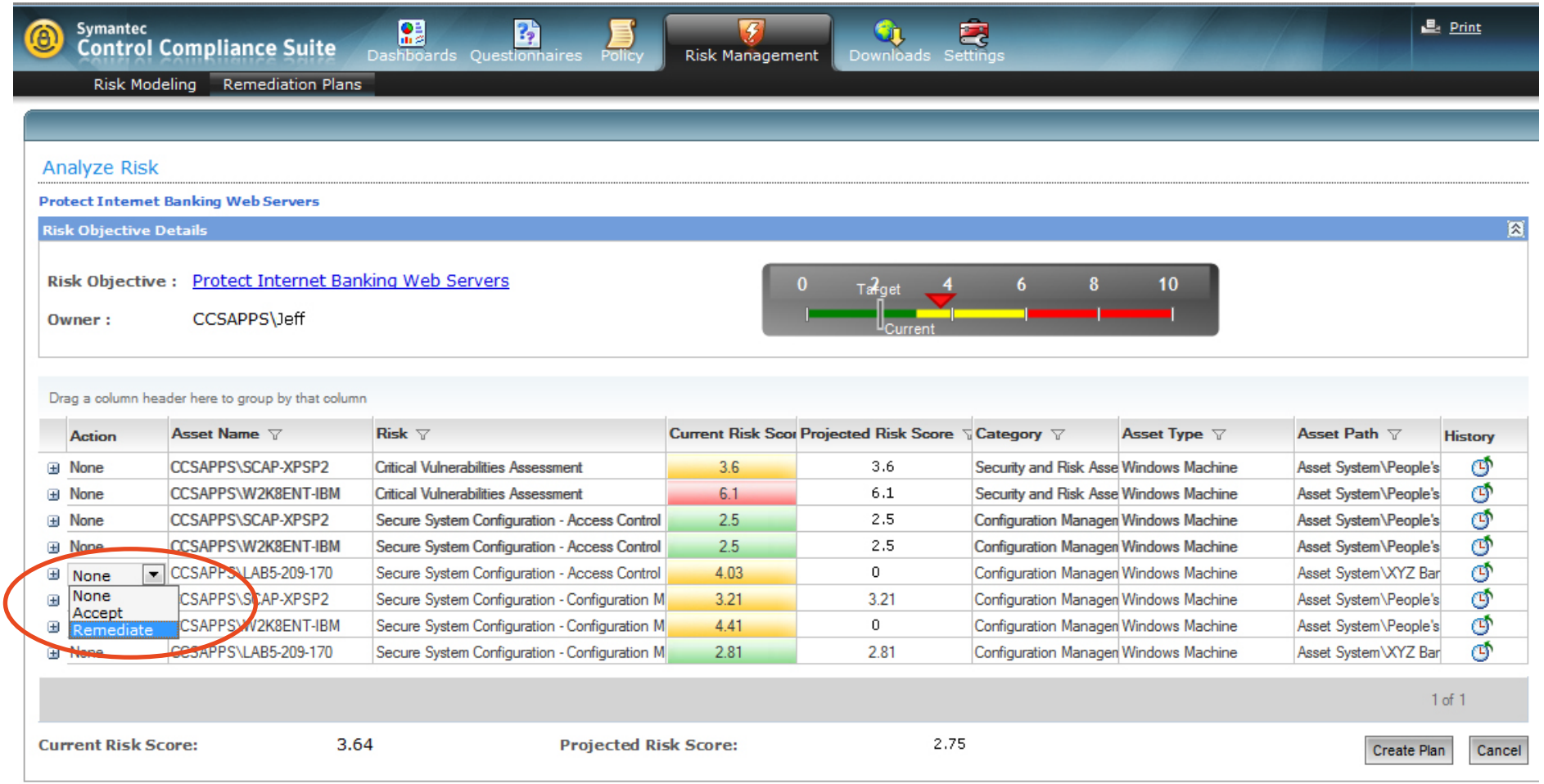
Enterprise Wide View of Business Risk

Visualize and Understand IT Risk

Balanced View of Business and Operational Metrics

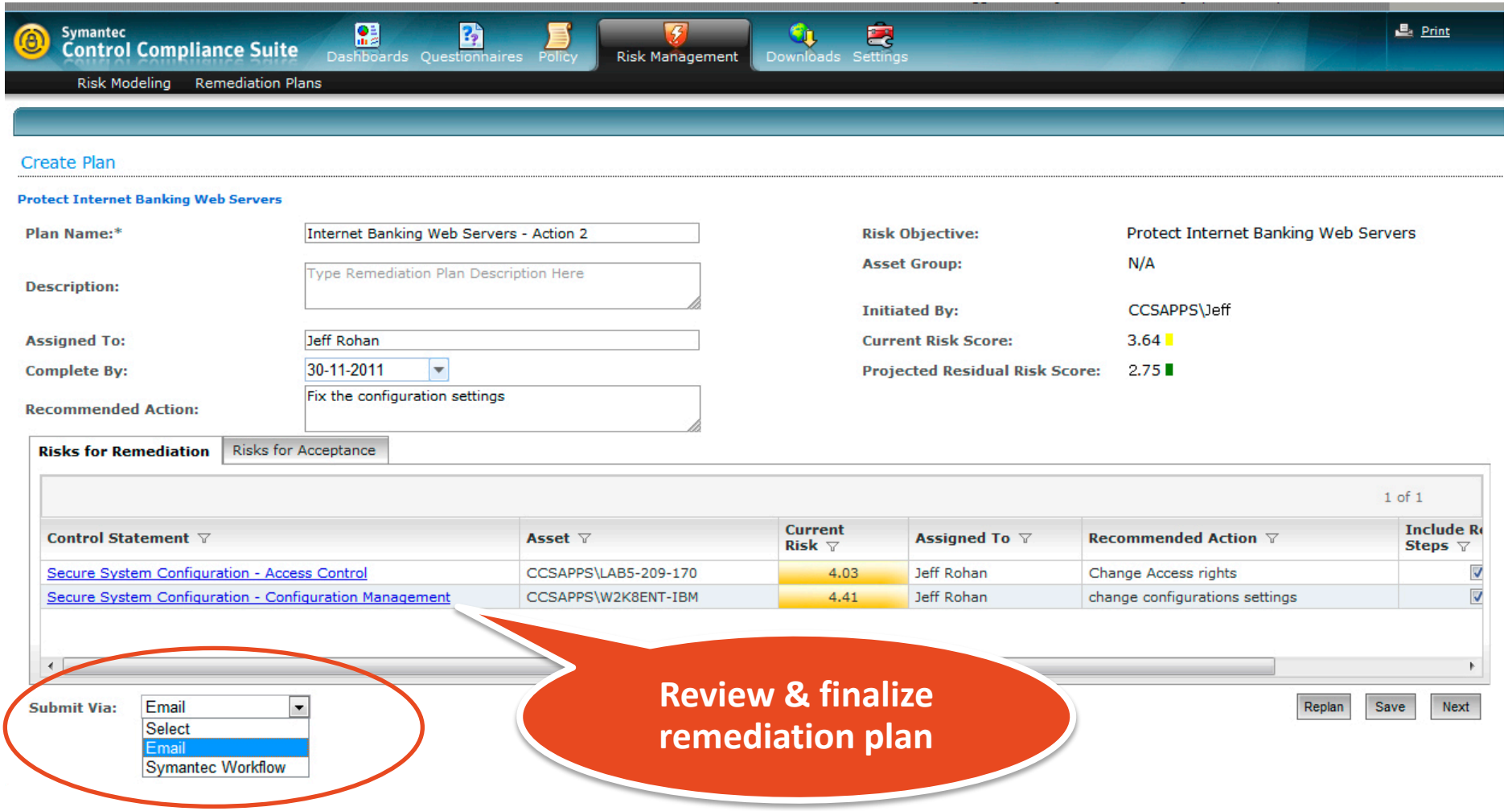
Prioritize Remediation Based on Risk

Risk Modeling



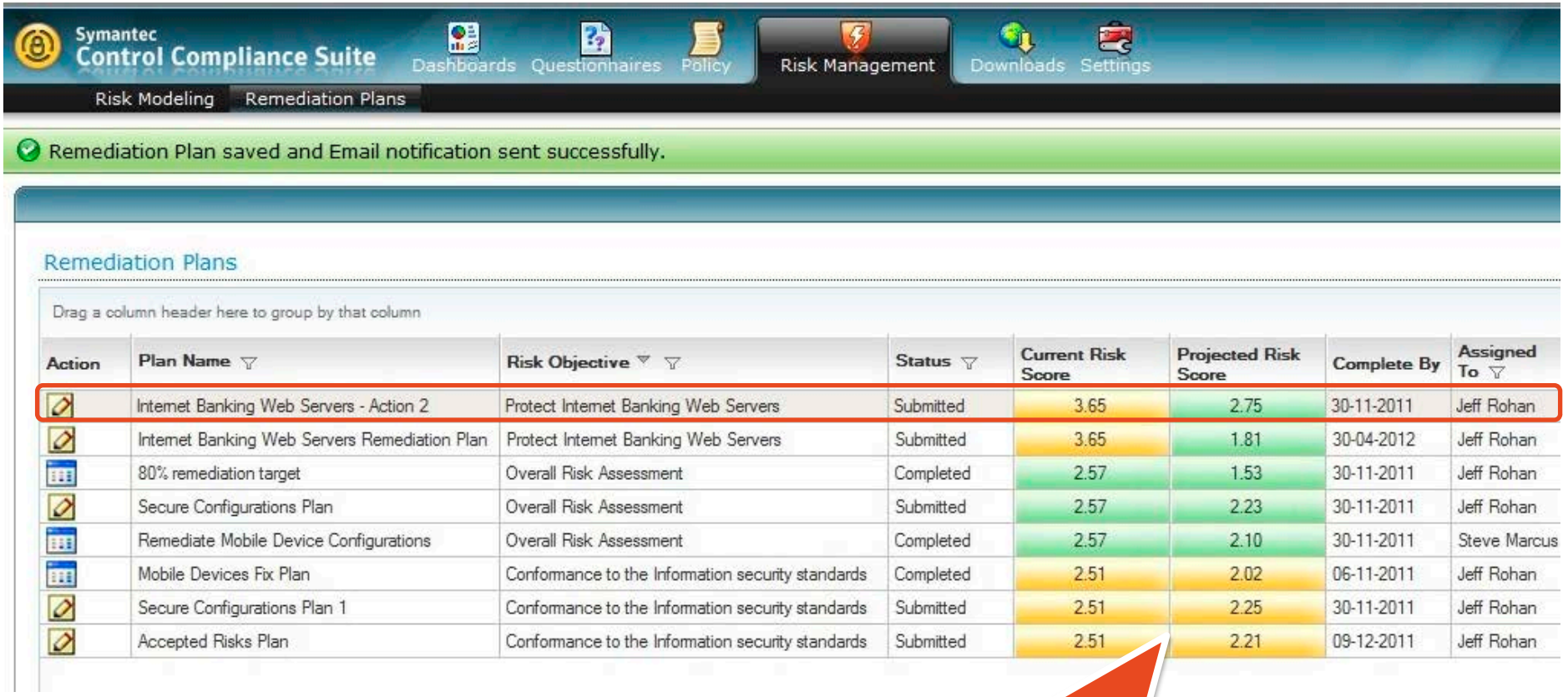
Prioritize Remediation Based on Risk

Remediation Plan by Risk Objective



Monitor Risk Reduction Over Time

Manage Remediation Plans



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 3rd 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!

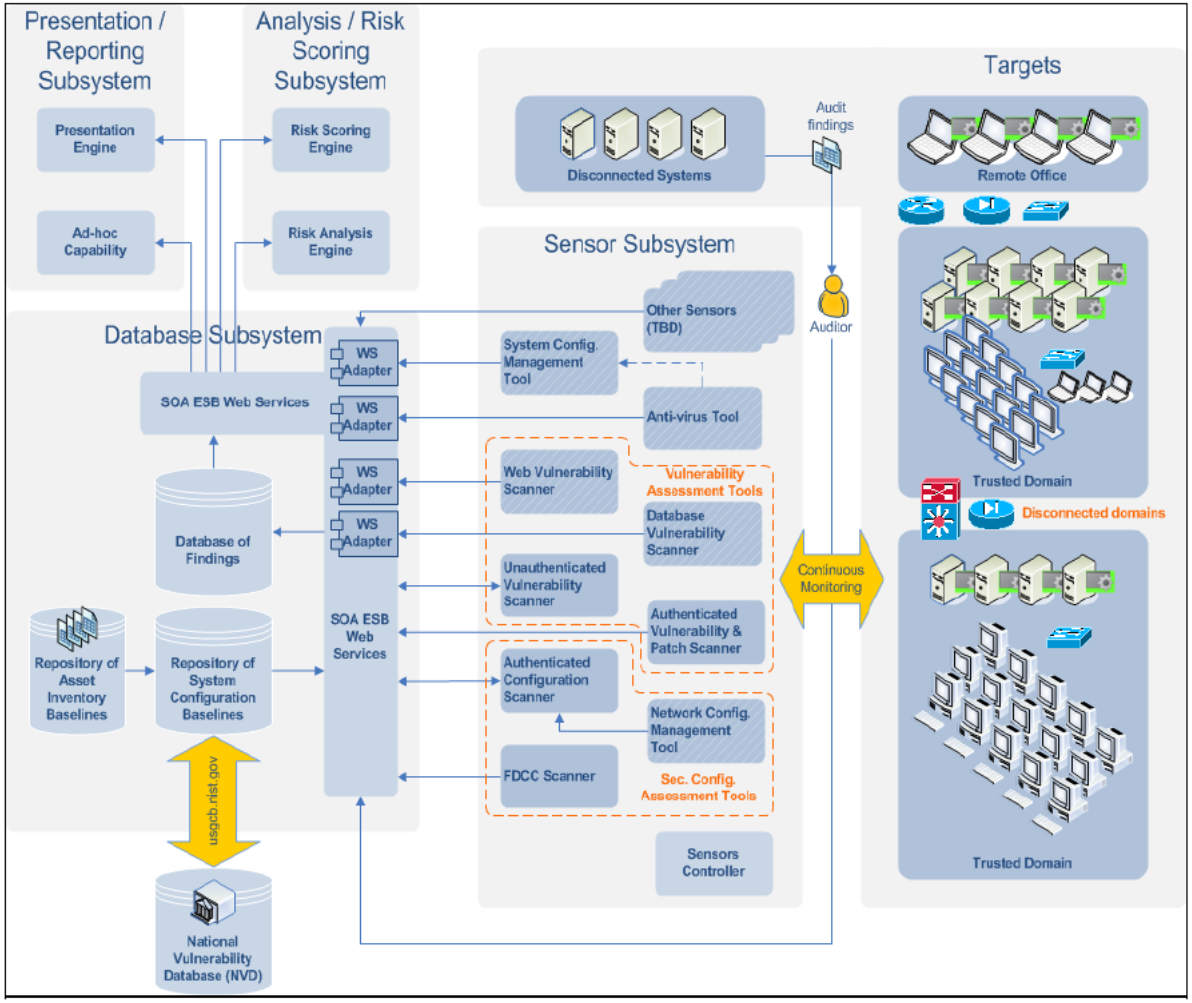


Figure 3. Contextual Description of the CAESARS System

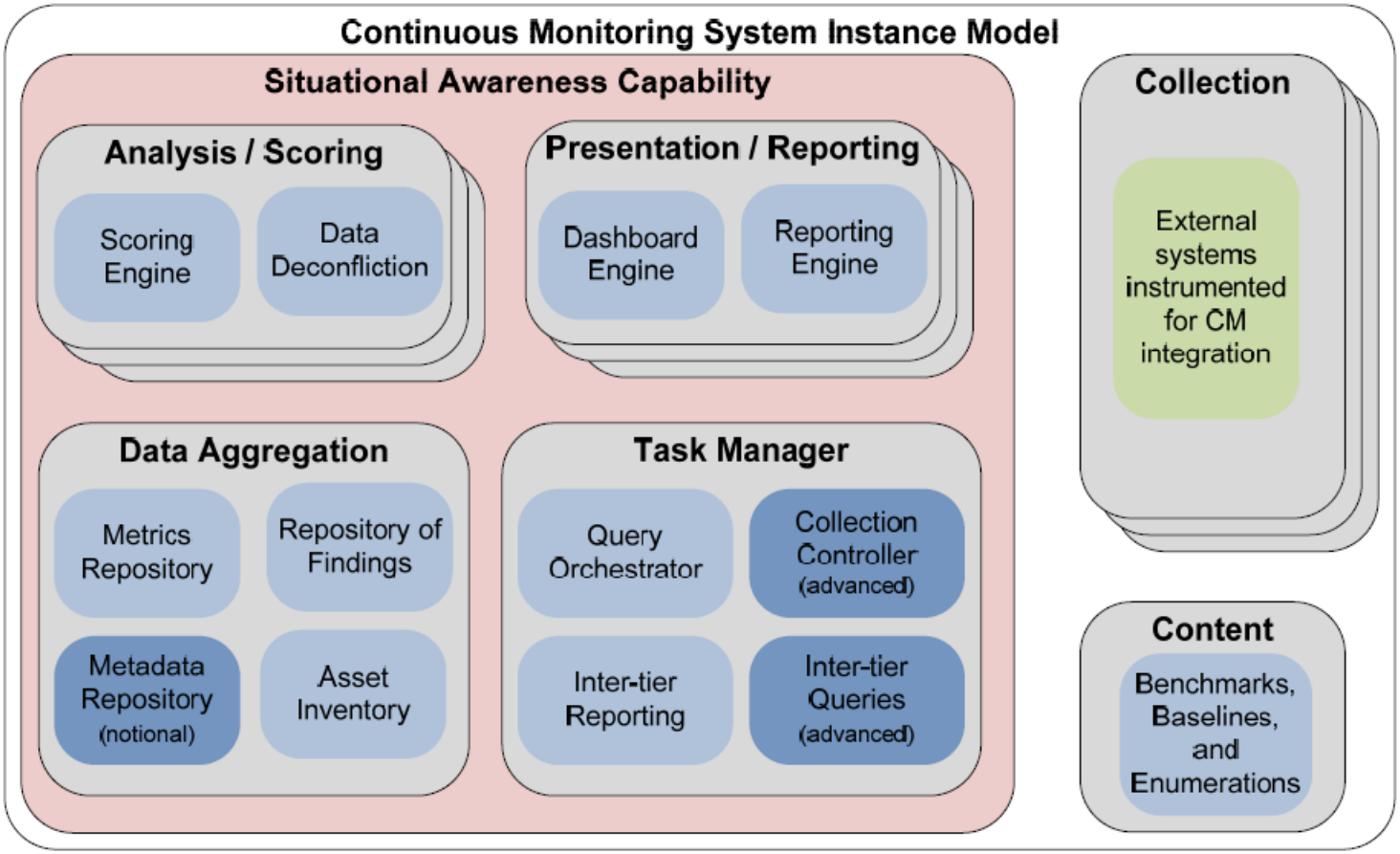
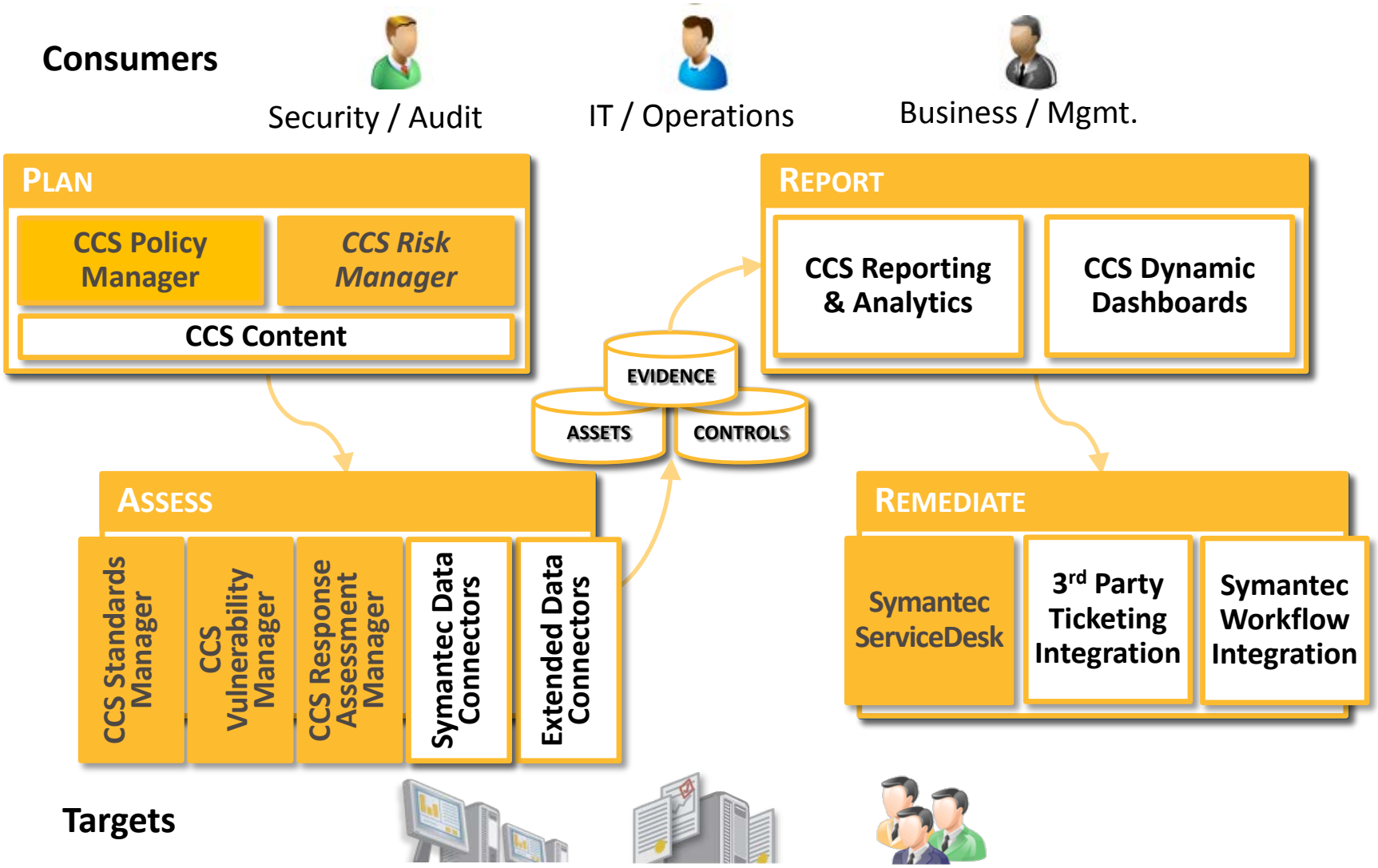


Figure 4. CAESARS Framework Extension Subsystems

Symantec Control Compliance Suite – Overview



** Planned new product. Roadmap subject to change.*

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.

** Planned new product. Roadmap subject to change.*