

# MetricStream

**MetricStream**

**GRC**

**SUMMIT 2013**

---

**MIDDLE EAST**

---

October 29 - 30, 2013 | Dubai, UAE

# Aligning IT, Security and Risk Management Programs

---

**Ahmed Qurram Baig,** CISSP, CBCP, CRISC, CISM  
Information Security & GRC Expert

**MetricStream**

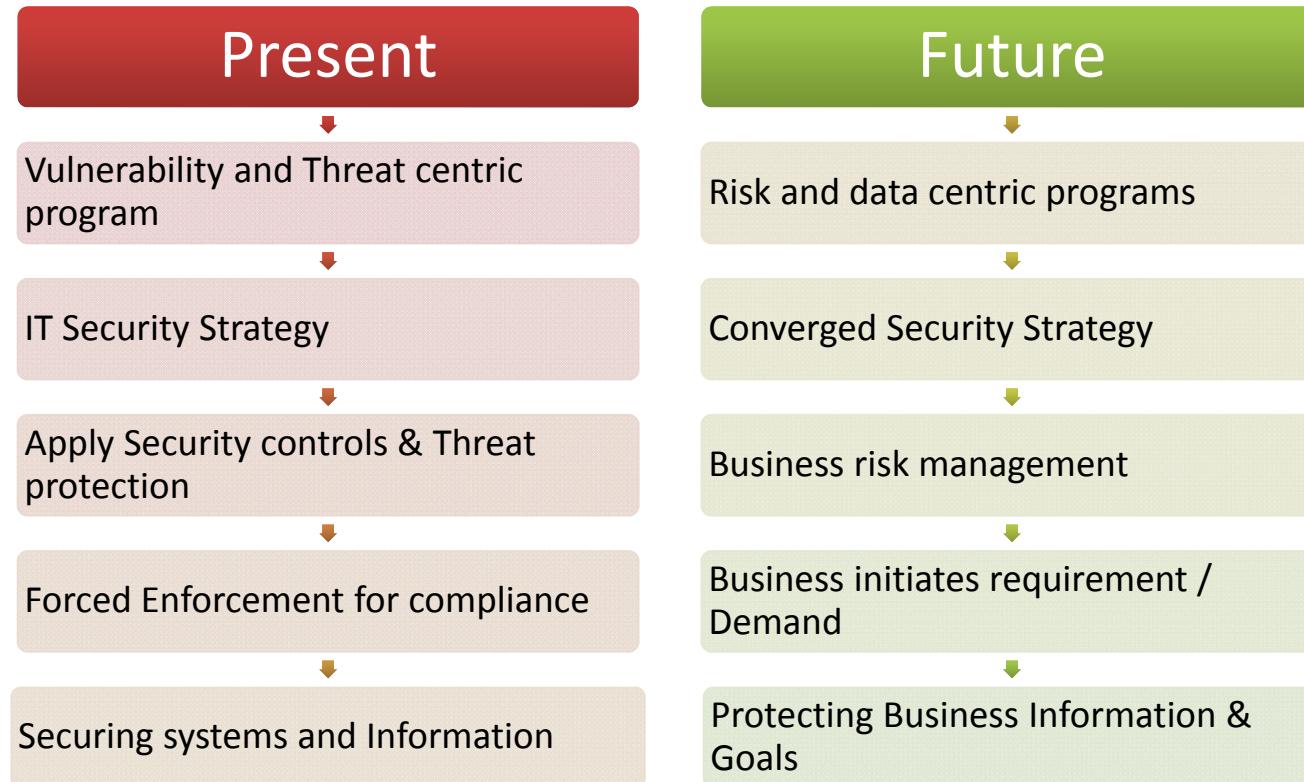
**GRC**  
**SUMMIT 2013**  
**MIDDLE EAST**

October 29 - 30, 2013 | Dubai, UAE

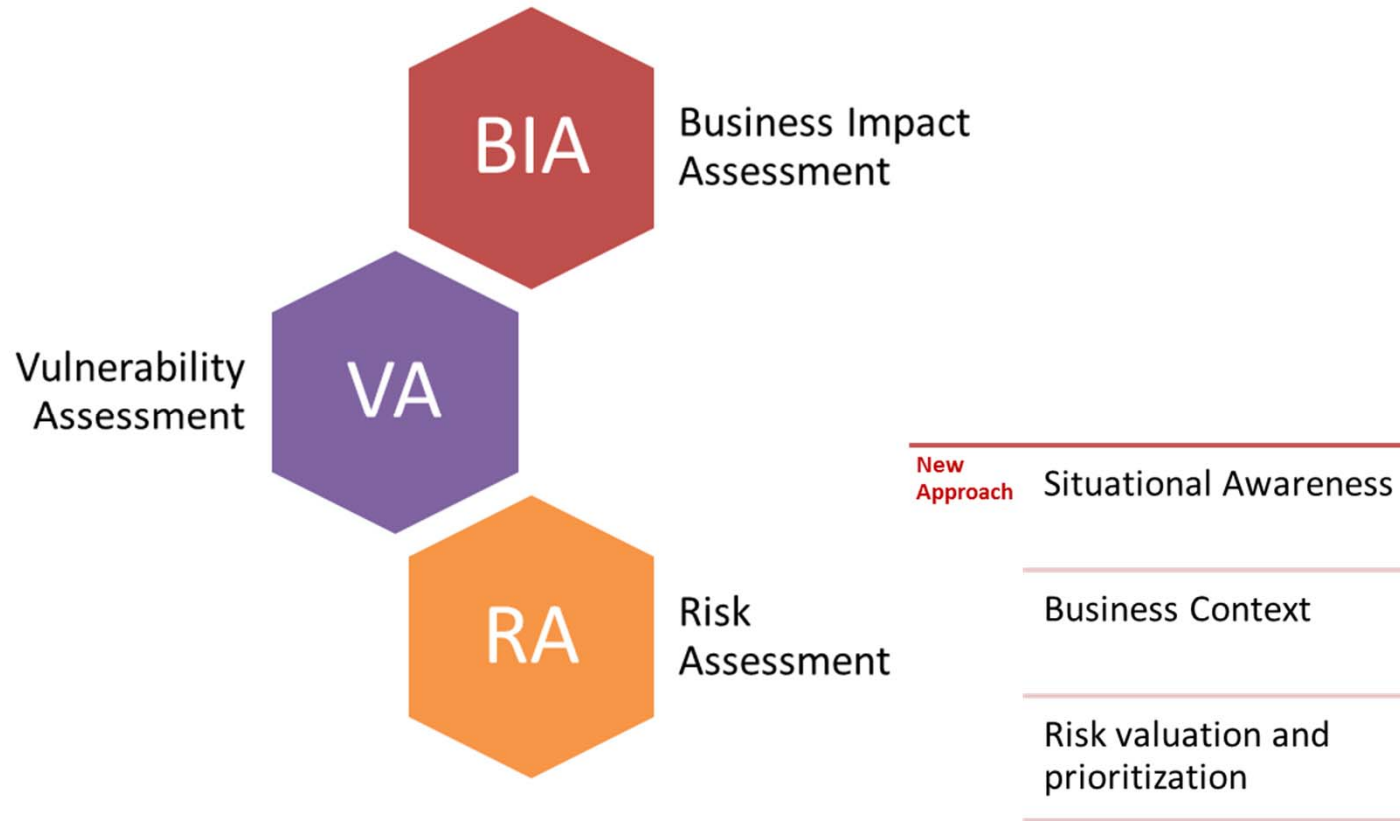
# Challenges to Risk Management & Governance

- Balancing extensive requirements originating from multiple governing bodies.
- Balancing legislation and company specific policy.
- Evolution to support different requirements and new legislation.
- Prioritizing available funding according to requirements introduced.
- More importantly fitting into the ERM program

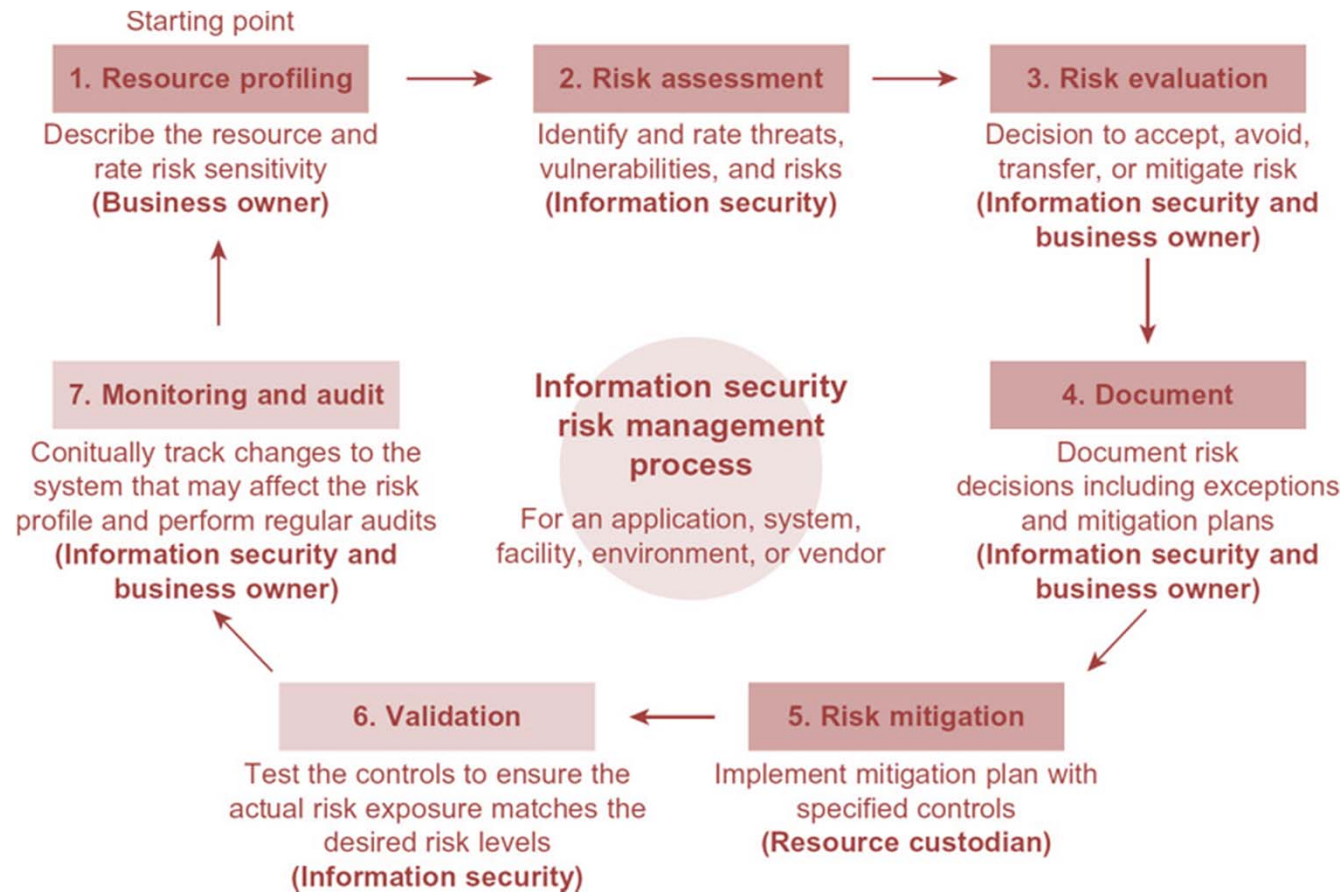
# IT Security to risk management mindset...



# Let's get this right ...

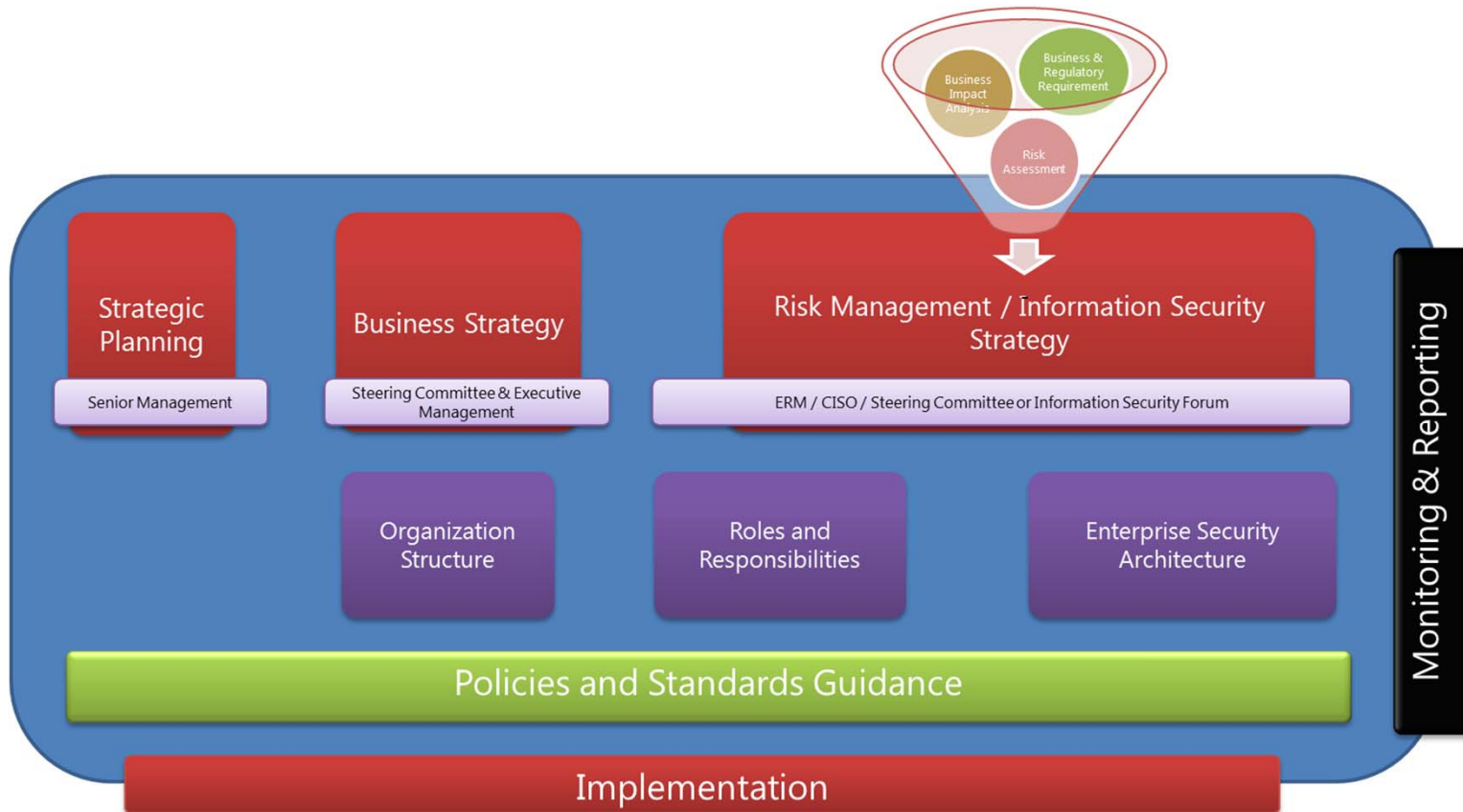


# Risk Management Lifecycle



Source: Risk Management Lifecycle, Evan Wheeler

# Information Security, Risk & Governance Framework



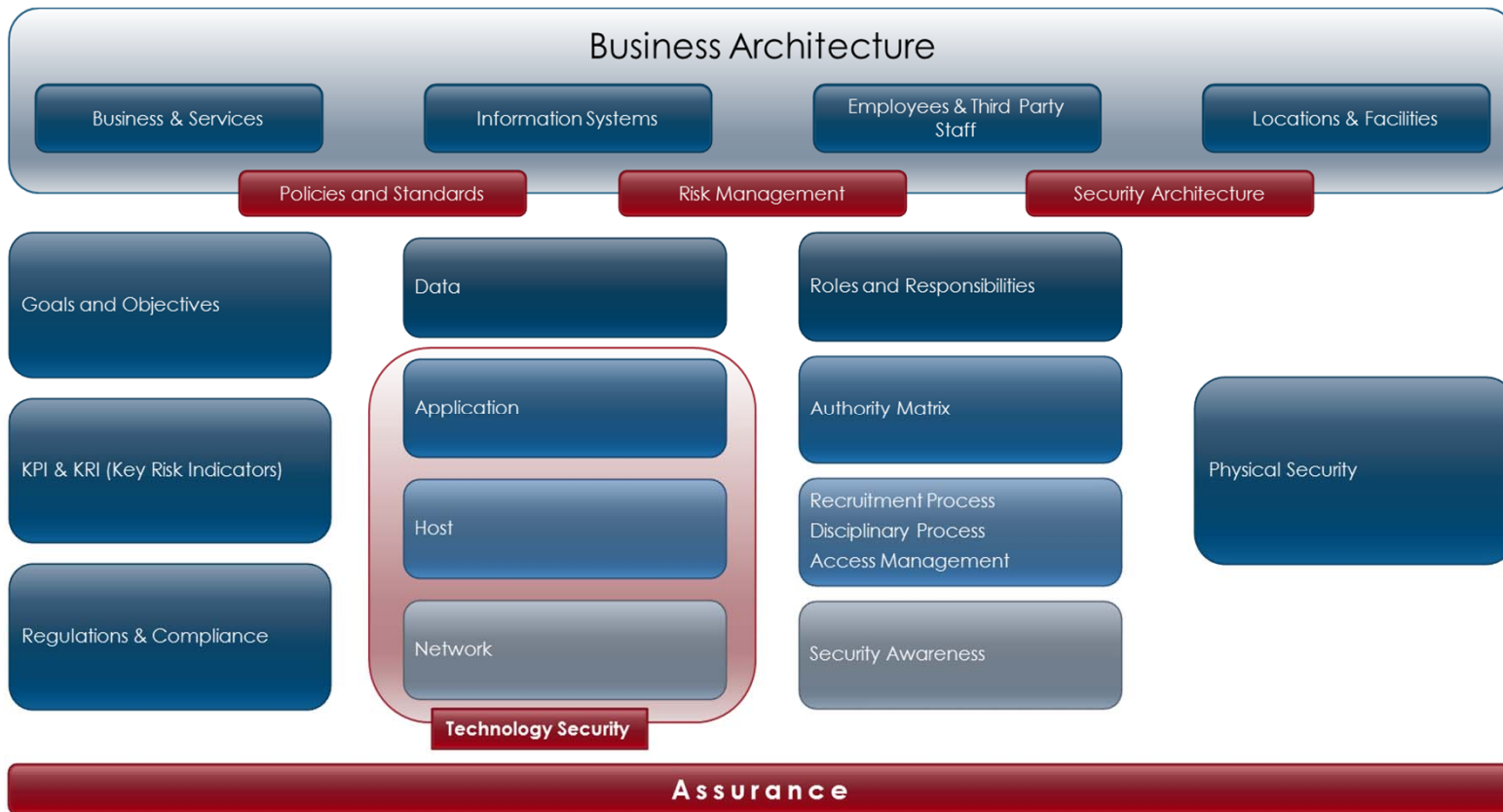
Ahmed Qurram Baig, Copyright, 2012.

[www.GRC-Summit.com/MEA2013](http://www.GRC-Summit.com/MEA2013)

MetricStream  
**GRC**  
SUMMIT 2013  
MIDDLE EAST  
October 29 - 30, 2013 | Dubai, UAE



# Enterprise Security Architecture & Risk Management



Ahmed Qurram Baig, Copyright, 2012.

# Information security & risk management activities



Ahmed Qurram Baig, Copyright, 2012.

[www.GRC-Summit.com/MEA2013](http://www.GRC-Summit.com/MEA2013)

MetricStream  
**GRC**  
SUMMIT 2013  
MIDDLE EAST  
October 29 - 30, 2013 | Dubai, UAE

# Benefits of effective risk management & governance

- Strategic Alignment
- Effective Risk Management
- Convergence & Business Process Assurance
- Resources Management:
  - Governance provides clarity of roles and responsibilities
  - Governance empower people responsible with authority
- IT Value Delivery
- Monitoring & Performance Measurement

# IT GRC Strategy

## Key Challenges:

- Reactive approach to IT Risk and Compliance – isolated risk and compliance initiatives and inability to align with business
- Lack of multi-perspective, 360 degree Risk Awareness – non-collaboration and lack of accountability on risk

## Ingredients for a successful IT GRC Strategy :

- Support and align with enterprise GRC strategy and architecture
- Common architecture across IT processes and architecture
- Integrated IT infrastructure to holistically address the IT GRC needs

## Essential components of IT-GRC Architecture:

Process Management

IT Risk and Security Management

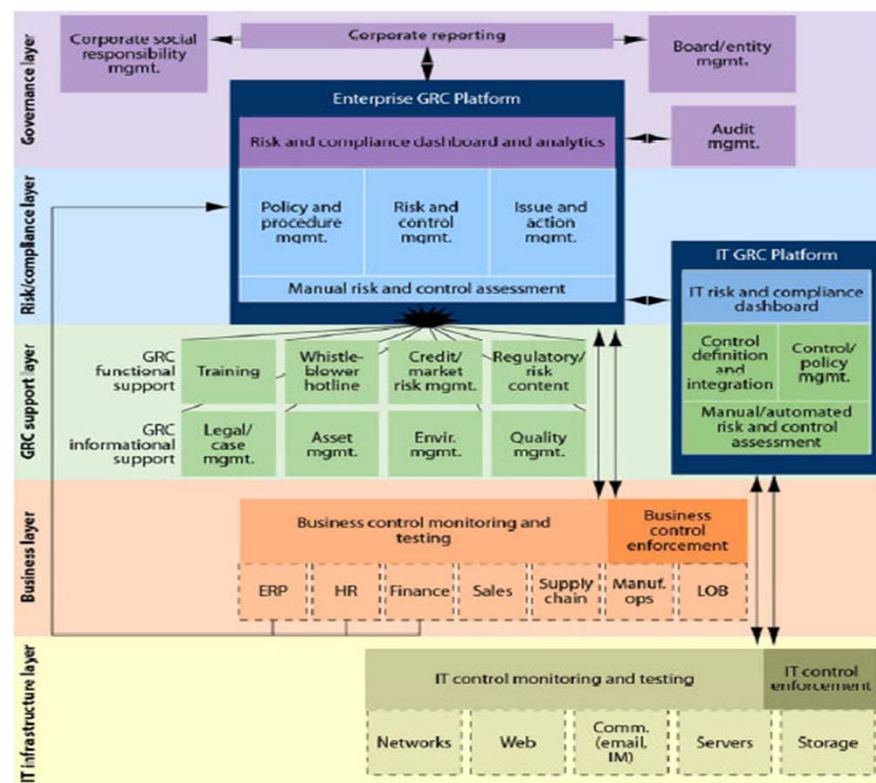
IT Compliance

Business Continuity Management

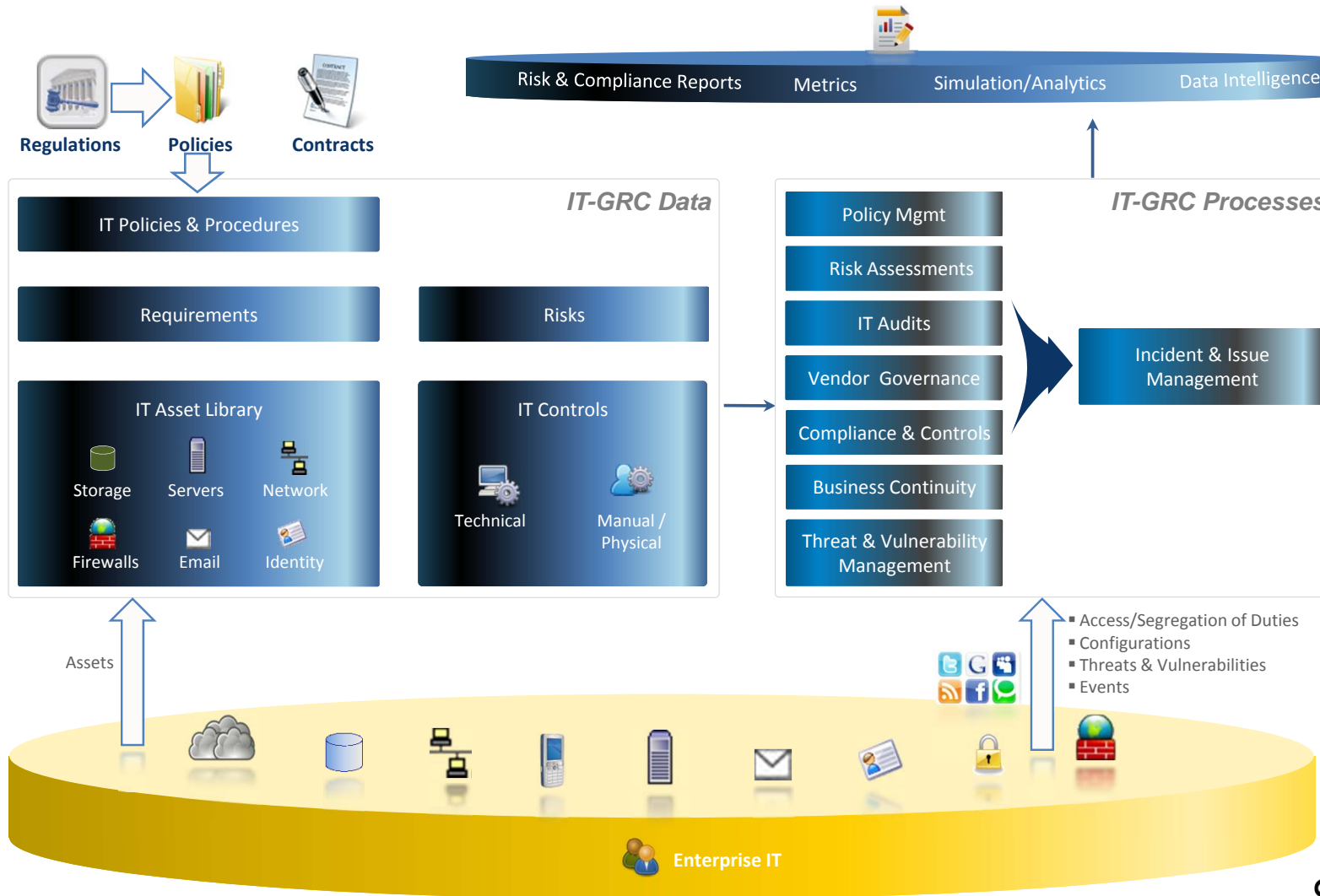
Policy & Content Management

Incident & Remediation Management

IT GRC Reporting, Metrics & Dashboard



Source: Forrester Report "The GRC Puzzle: Getting All The Pieces To Fit"



## Bottom-up Information Security

- TVM – Integration & Correlation Across Security Operations
- Security Intelligence
- Social Media Risk Intelligence
- Cloud Security
- Integrations: CMDB, VA, SIEM, DLP, etc.

## Bottom-up IT-Risk

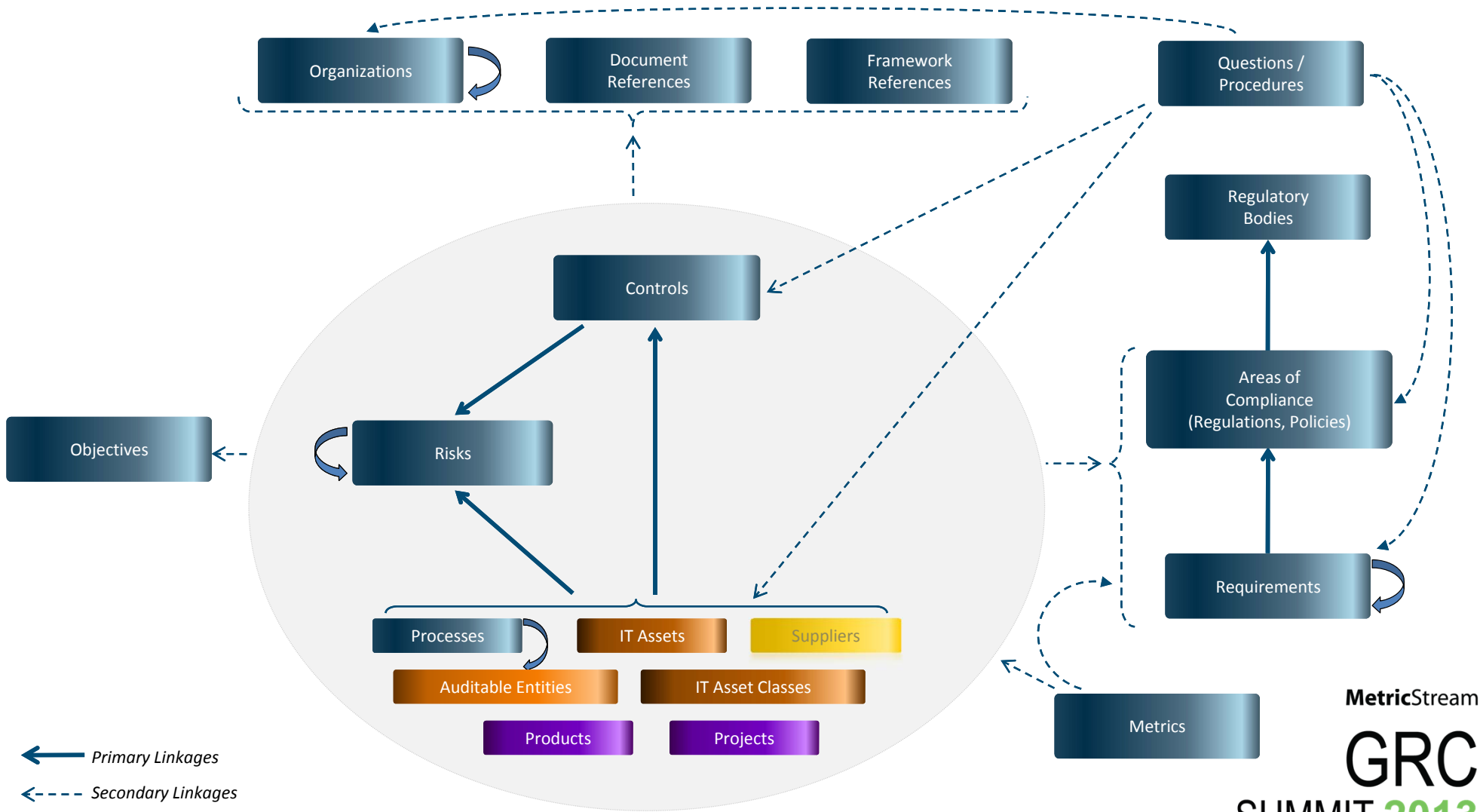
- Standardizing Risk Calculations & Analysis
- Implementing Risk Frameworks – ISO, NIST, COBIT, FAIR
- Integrated Risk Mgmt – InfoSec, IT-Ops, Compliance
- Controls Monitoring & Testing
- Risk Analytics



## Bottom-up IT Compliance

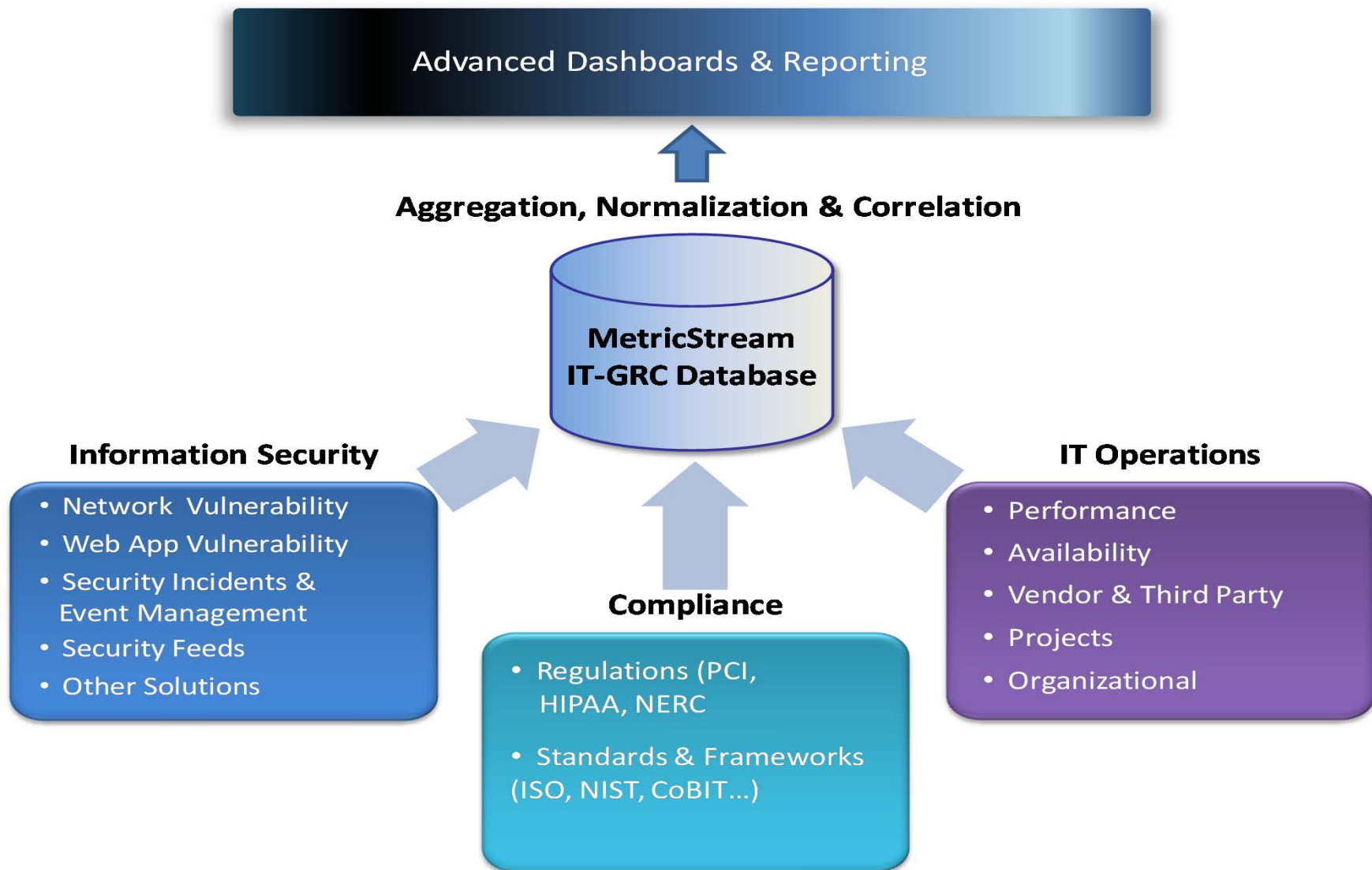
- Harmonized Controls
- Regulations: PCI, SSAE 16, FDIC, NERC, HIPAA
- Policy Compliance – Acceptance, Training, etc.
- Control Assessments
- Linking Policies to Control Objectives

## Integrated GRC

- Enterprise Risk Management – Common Risk & Control Framework
- Integrated Compliance and Controls
- Common Platform for Managing Risks & BCP
- Single Enterprise Platform for ALL GRC Initiatives



 Primary Linkages  
 Secondary Linkages





# MetricStream IT GRC Solution – Key Benefits

- Automation and rationalization of risk management processes with support for federated risk analysis within units
- A common IT risk and control framework, tied to business risks
- Visibility in risks, risk factors, mitigating controls, metrics and analytics with rich context, and integration with IT and security systems
- Automated and streamlined issue and remediation management
- Extensive support for standards & frameworks: ISO, COBIT, FAIR, NIST
- Advanced Analytics – e.g.: Monte Carlo Simulation or Bayesian analysis to prioritize remediation efforts

# Risk Reports & Heatmaps

**MetricStream** Welcome: Gulden Yuncuoglu My Tasks: 0 [0 New, 0 Past due] My Calendars My Profile | Help | Logout

**Risks** My Reports Administration Universal Search

Manage Assessments Setup Assessments Heat Map

---

**Heat Map**

TEB Risk Assessment Heat Map

		Likelihood						
		Very Low	Low	Low / Medium	Medium	Medium / High	High	Very High
		1	2	3	4	5	6	7
Impact	Low	1	Green	Green	Green	Yellow	Yellow	Orange
	Medium	2	Green	Green	Green	Yellow	Yellow	Orange
	High	3	Green	Green	Yellow	Yellow	Orange	Orange
	Very High	4	Green	Yellow	Yellow	Orange	Orange	Red

**Applications/Services Risk Report** Filters Done

Report Data as of: 08/08/2013 02:30 PM

Risk Name	Business ...	Risk Rating	LastASSE...	LastASSE...
Application Name: TEB Application/Service #2				
		Medium	6	
TEB Mapping Employee IDs to Applicati...		7	07-Aug-2013	Ferhat Arpaci
TEB Maker Checker Approval Process ...		5	07-Aug-2013	Ferhat Arpaci
TEB Integration with TEBKEYS IAMS		6	07-Aug-2013	Ferhat Arpaci
TEB User Records Data Management		6	07-Aug-2013	Ferhat Arpaci
Application Name: TEB Application/Service #4				
		Medium	5	

---

**MetricStream** Welcome: Gulden Yuncuoglu My Tasks: 0 [0 New, 0 Past due] My Calendars My Profile | Help | Logout

**Risks** My Reports Administration Universal Search

Manage Assessments Setup Assessments

---

**Manage Assessments**

Create/Manage Assessments

Risk Assessment Plan

Risk Assessment Task

Page 1 of 1

**Top-10 Risky Applications/Services**

Overall Risk Rating for the Application/Service

TEB Application/Service Name	Overall Risk Rating
TEB Applicati on/Servi ce #7	8
TEB Applicati on/Servi ce #3	7
TEB Applicati on/Servi ce #6	6
TEB Applicati on/Servi ce #1	6
TEB Applicati on/Servi ce #9	6
TEB Applicati on/Servi ce #2	6
TEB Applicati on/Servi ce #4	5
TEB Applicati on/Servi ce #10	4
TEB Applicati on/Servi ce #5	3
TEB Applicati on/Servi ce #8	3

**Search Reports**

Assessment Report

Risk Assessment Status Report

Page 1 of 3

**Applications/Services Risk Report**

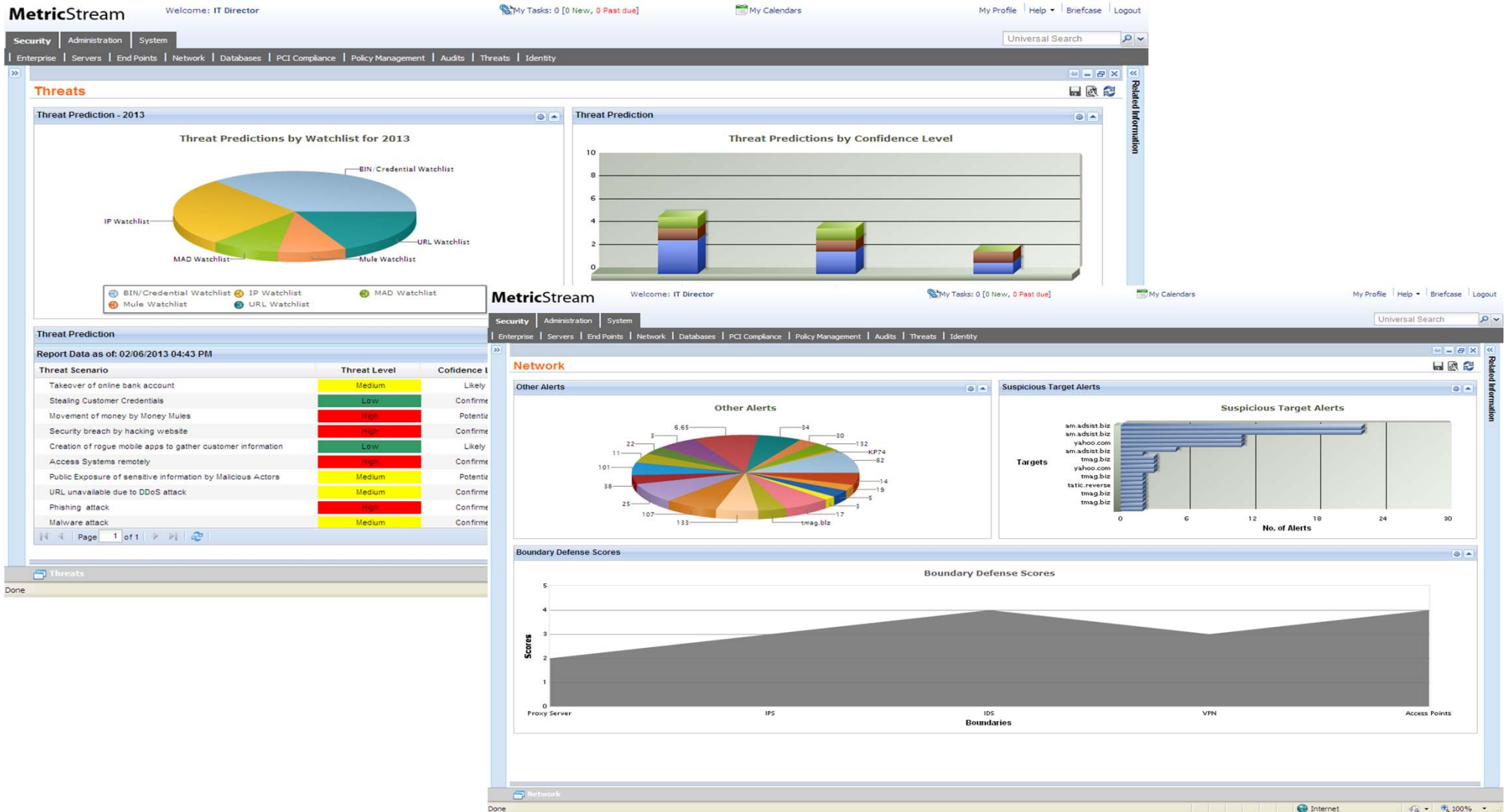
Risk Name	Business Cri...	Risk Rating	Last Assess...	Last Assess...
Application_name: TEB Application/Service #1				
		Medium	6	
TEB User Records Data Management		7	07-Aug-2013	Ferhat Arpaci
TEB Mapping Employee IDs to Application Use...		10	07-Aug-2013	Ferhat Arpaci
TEB Maker Checker Approval Process for Us...		6	07-Aug-2013	Ferhat Arpaci
TEB Integration with TEBKEYS IAMS		5	07-Aug-2013	Ferhat Arpaci
Application_name: TEB Application/Service #10				
		Low	3	
TEB User Records Data Management		4	07-Aug-2013	Ferhat Arpaci
TEB Mapping Employee IDs to Application Use...		3	07-Aug-2013	Ferhat Arpaci

Page 1 of 2

Displaying records 1 - 20 of 40

Powered by MetricStream

# Threat & Security Posture Reports



# Thank You

## Q & A