Next Generation Policy & Compliance

Mason Karrer, CISSP, CISA

GRC Strategist - Policy and Compliance, RSA

Core Competencies – C33

ISACA®

Trust in, and value from, information systems

San Francisco Chapter

Introductions...

- Mason Karrer **CISSP, CISA**
  - GRC Strategist, Policy and Compliance
  - Solution Management & Direction
  - Archer Content Operations
- Past Experience:
  - Practitioner for 15 years
  - Software Development & IT
  - Security & Audit

ISACA®

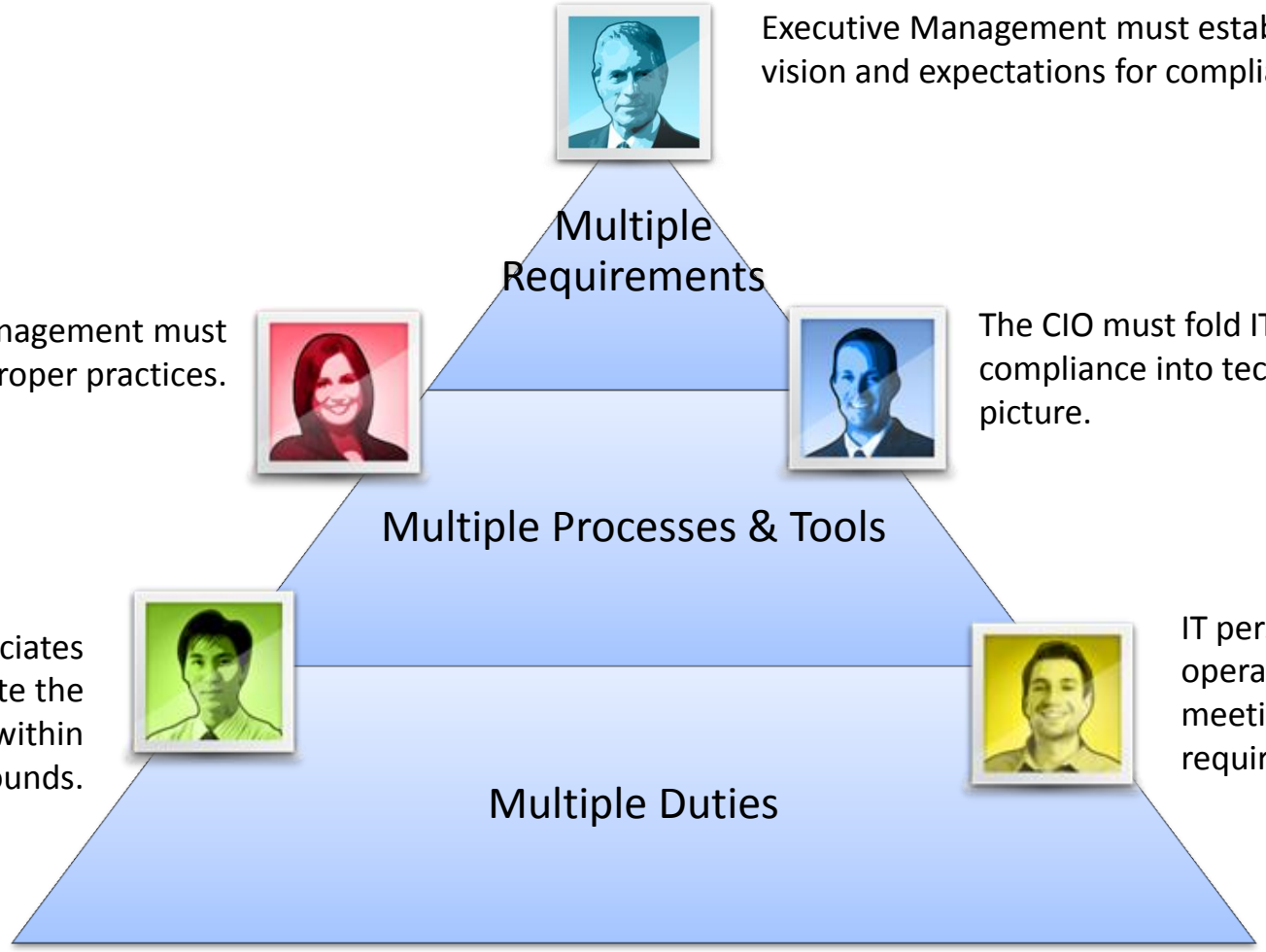
Trust in, and value from, information systems

San Francisco Chapter

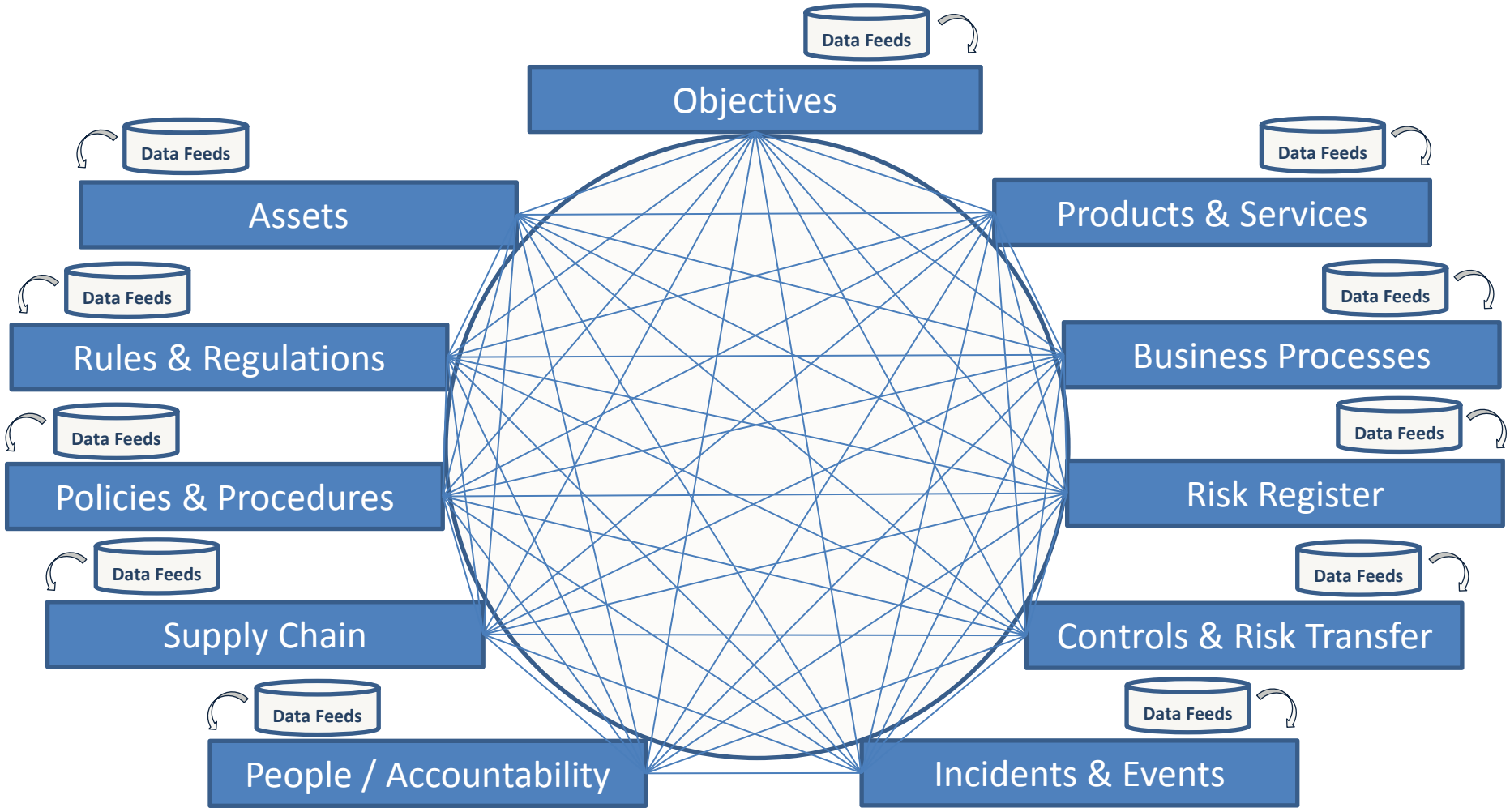
Overview

- Policy and compliance challenges
- Regulatory hurdles & consequences
- Policy and compliance in the new era

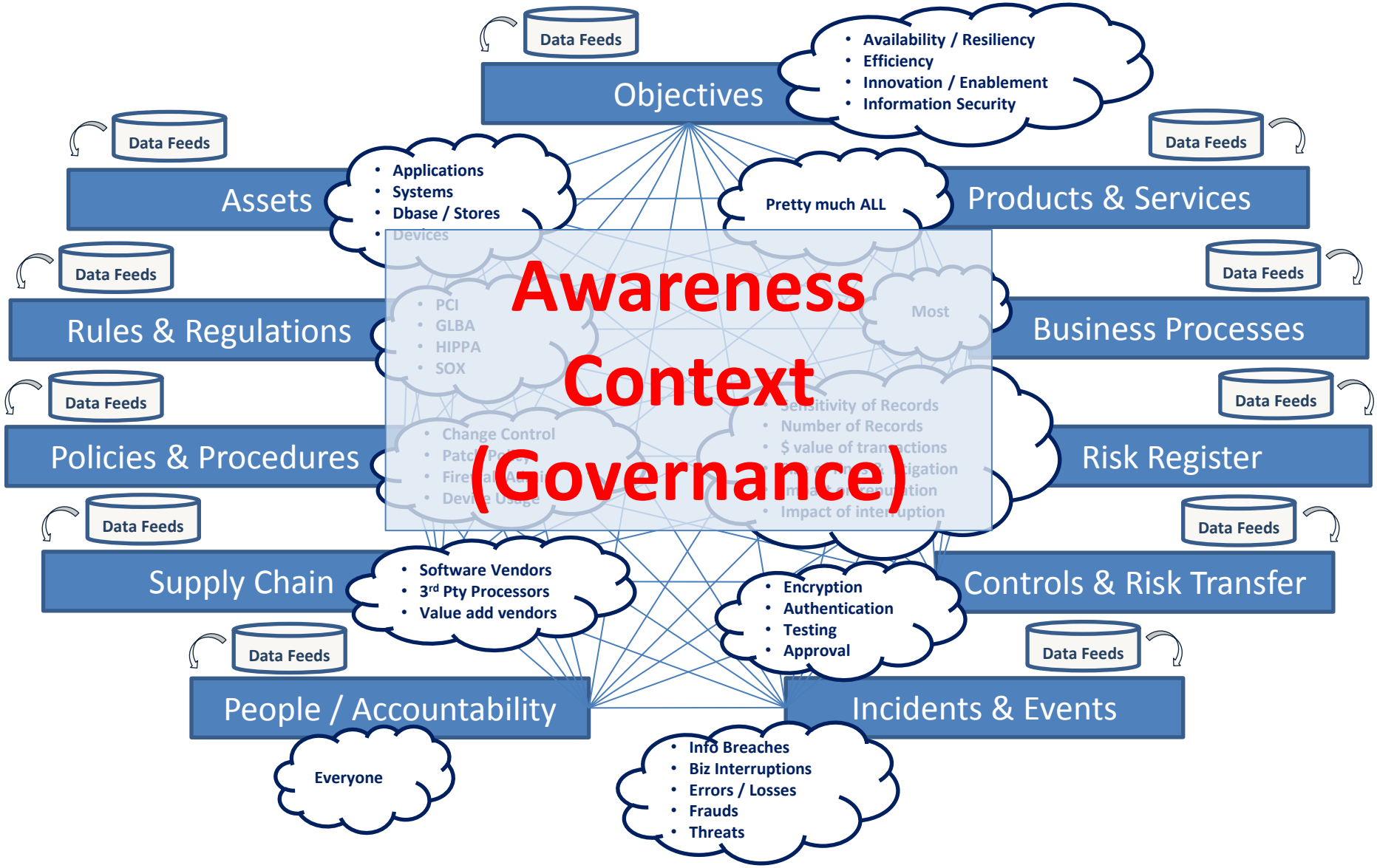
Today's Policy and Compliance Challenges…



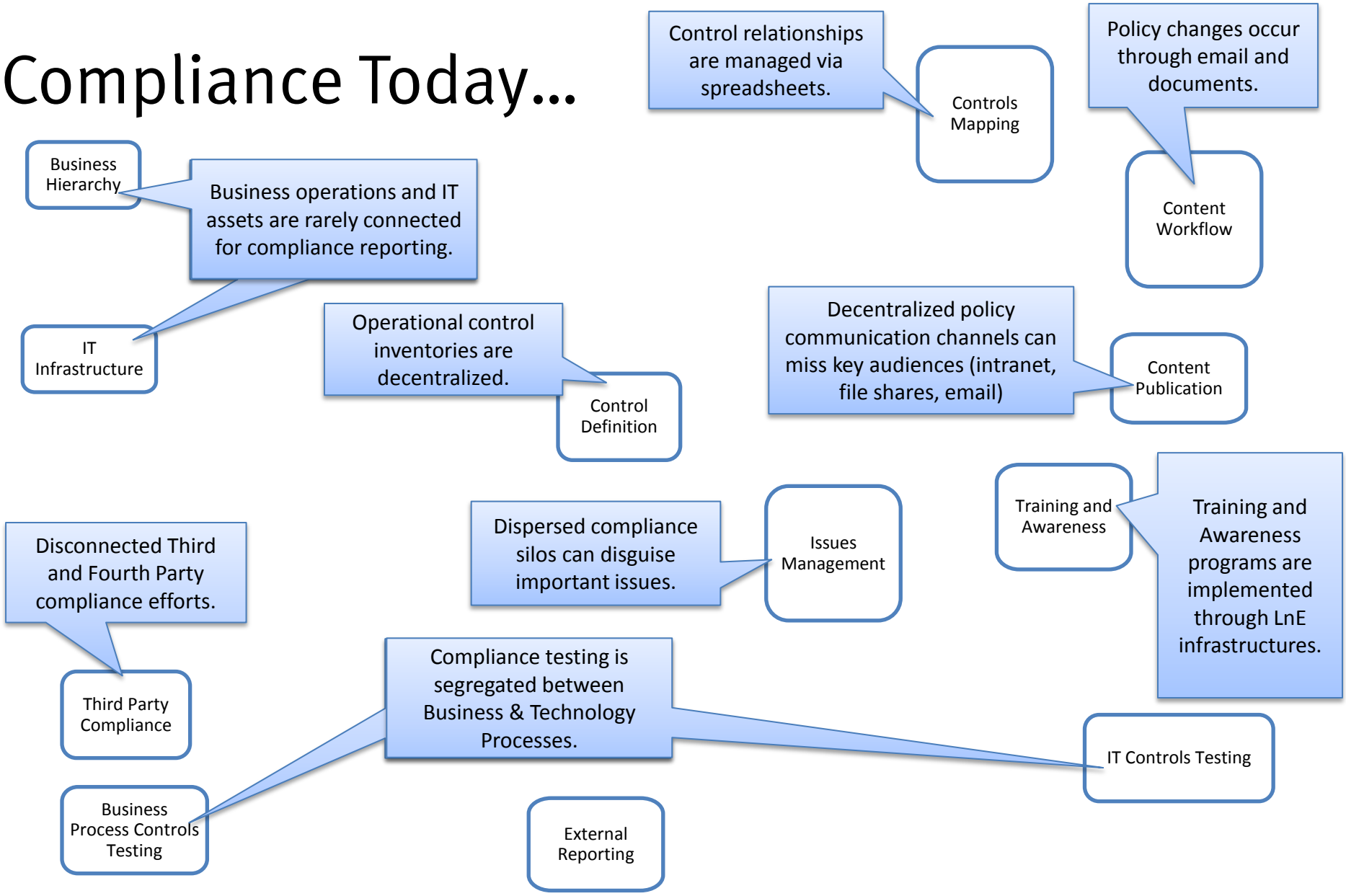
Typical Information Architecture



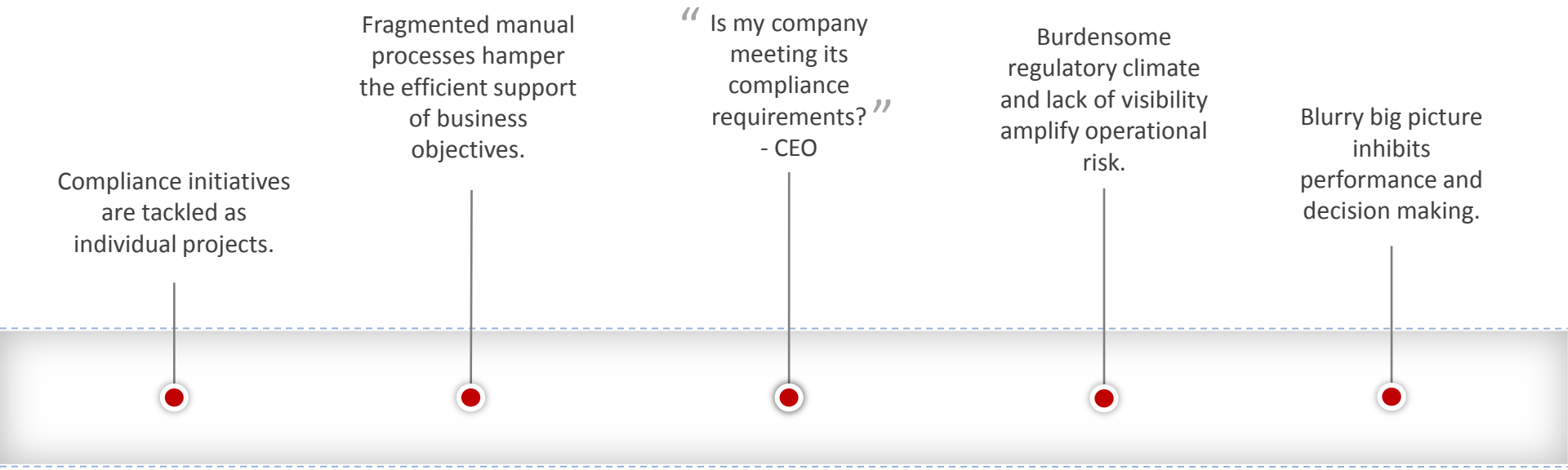
Typical Information Architecture



Compliance Today…

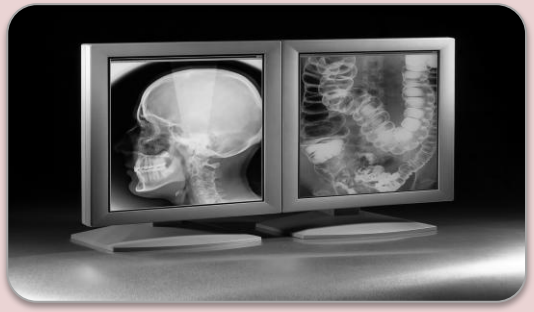


Consequences…



Regulatory "Motivation"...

Affecting the bottom line across industries



$2.8B

81%

9000+

Regulatory "Motivation"...

Affecting the bottom line in financial services

$2.8B

- FY2011: 735 SEC enforcement actions **(9% increase from 2010)**
- $2.8B in penalties and disgorgements
- Morgan Stanley had better success

Regulatory "Motivation"...

Affecting the bottom line in the utility sector

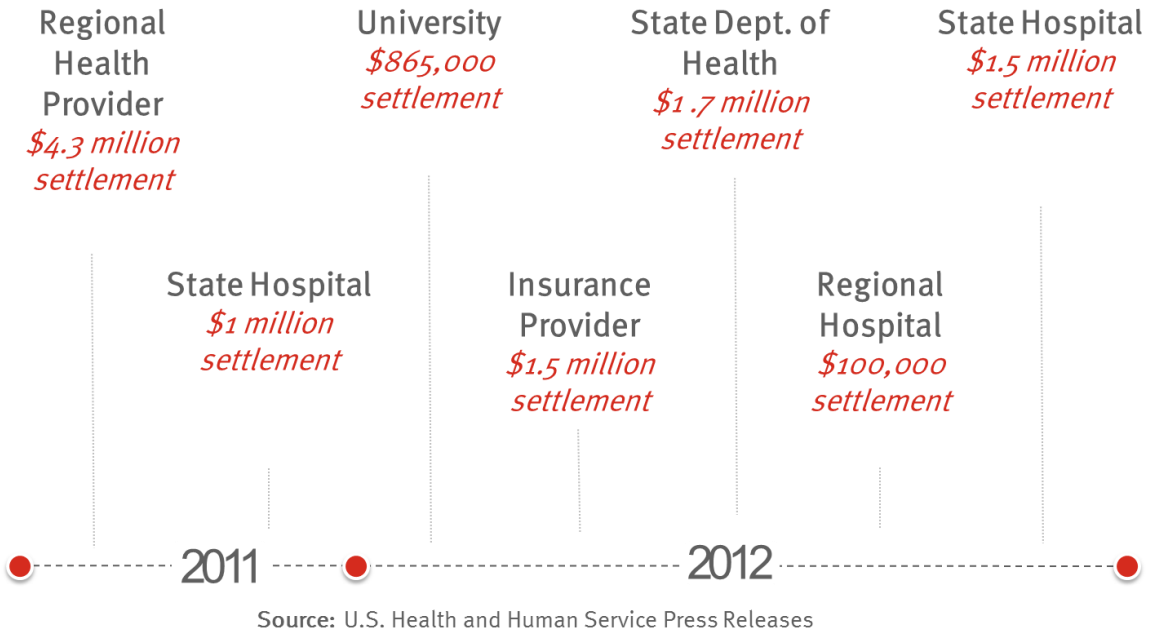
81%

- FY2012 YTD: 842 penalty notices issued
- $91M in penalties issued
- 81% CIP related - 23% ranked "High"

Regulatory "Motivation"...

Affecting the bottom line in healthcare

9000+ HIPAA privacy complaints in 2011.



Source: U.S. Health and Human Service Press Releases

Elements of a Next Gen P&C Portfolio

Guiding Principles

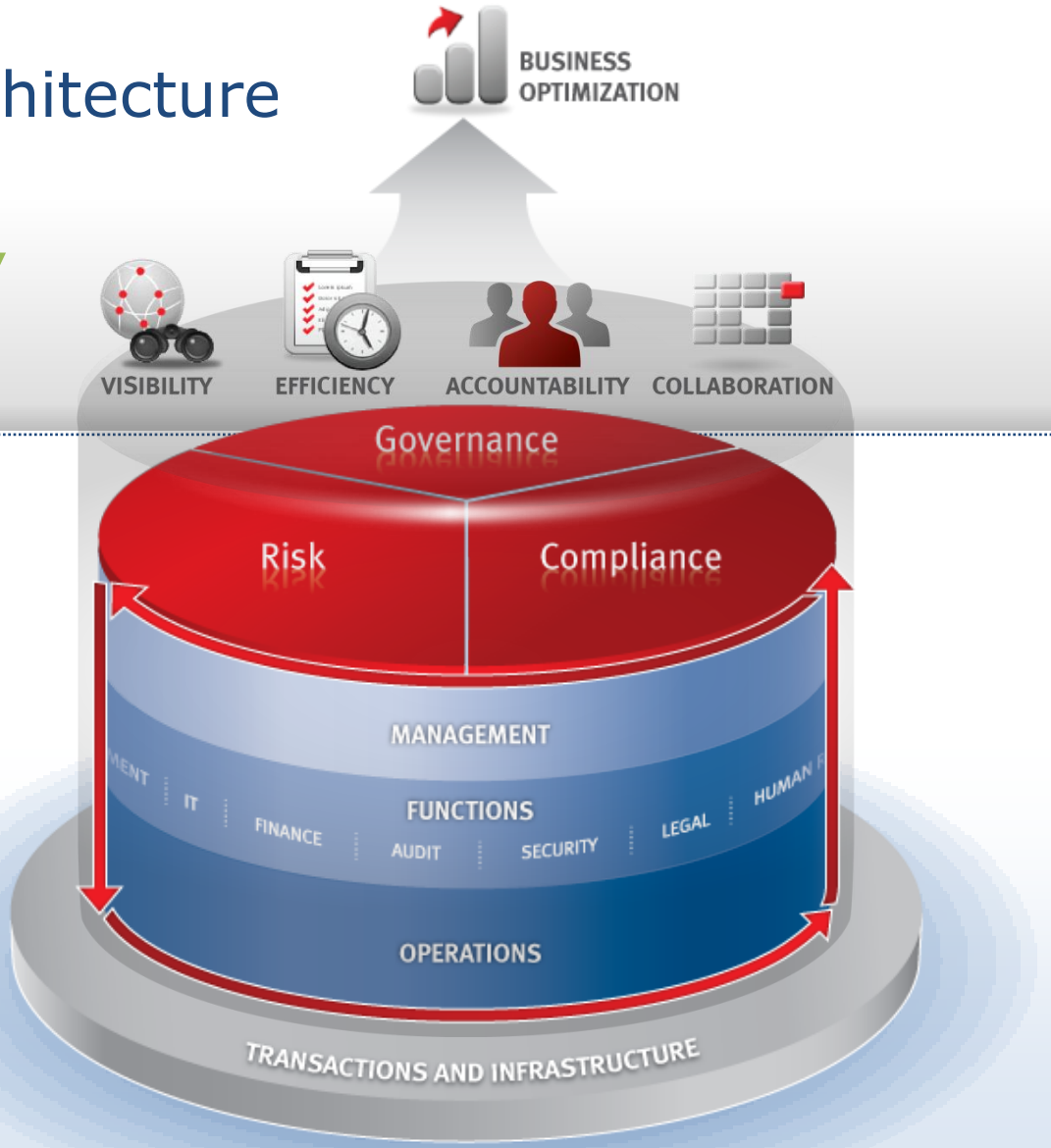
- Transparency
- Security & Peace of Mind
- Consistency & Sustainability
- Agility & Proficiency
- Balanced Effort vs. Reward

Objectives

- End to End Coverage
- Clarified Ownership
- Information Integration
- Flexible & Easy to Use
- Efficiency & Unified View

RSA GRC Reference Architecture

Visibility, Efficiency, Accountability, & Collaboration



Our Approach - 50,000 ft. View

Governance

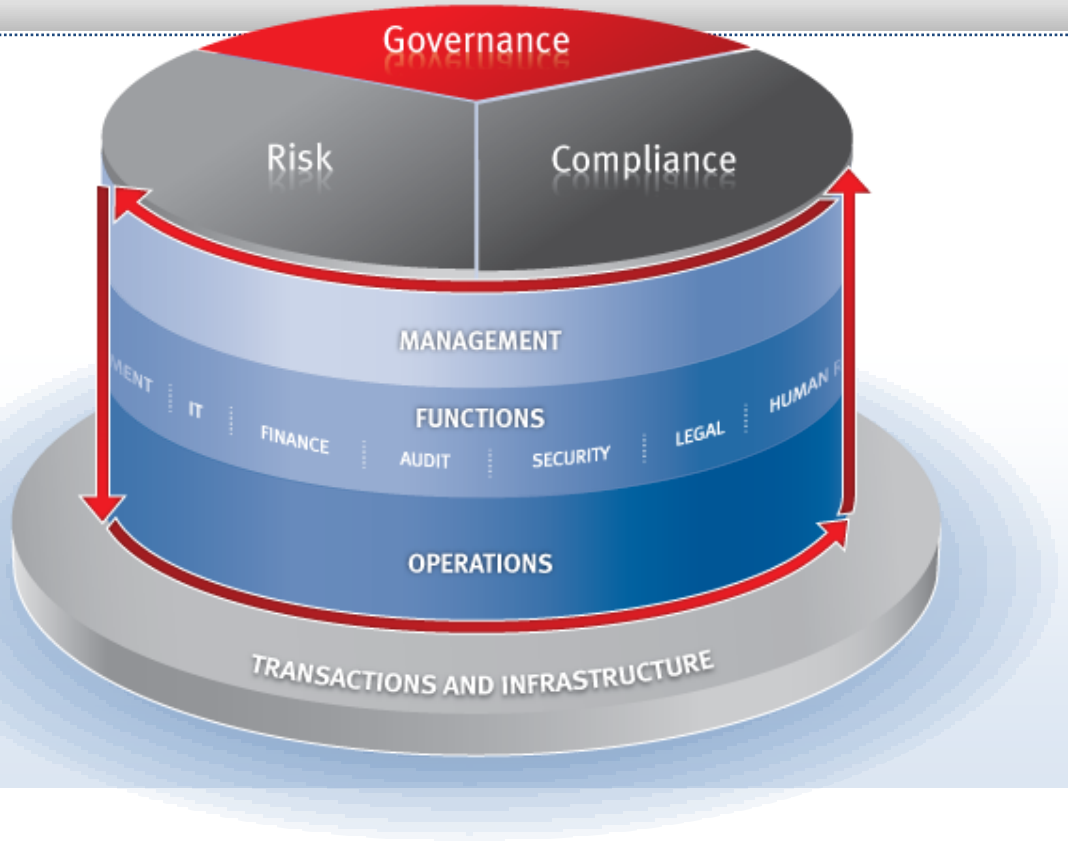
Description of the organization, its business assets and asset ownership and relationships as well as definition of prescribed business practices

Key Processes:

- Process Management
- Enterprise Management
- Strategy Management

Key capabilities

- **Asset Awareness**
- Organizational Hierarchy
- **Controls Mapping and Rationalization**
- Policy & Standards Creation and Publication
- Delegated Authorities
- Role Management
- Strategic Planning



Our Approach - 50,000 ft. View

Risk

Identification, management and tracking of issues that could adversely affect the business

Key Processes:

- Enterprise Risk Management
- Third Party Management
- Event Management

Key capabilities

- Risk Assessment
- Financial Risk Management
- **IT Security Management**
- BCM/DR
- Matters Management
- Crisis Management
- **Third Party Risk Management**
- KRIs

Our Approach - 50,000 ft. View

Compliance

Assurance that the business is adhering to defined business practices.

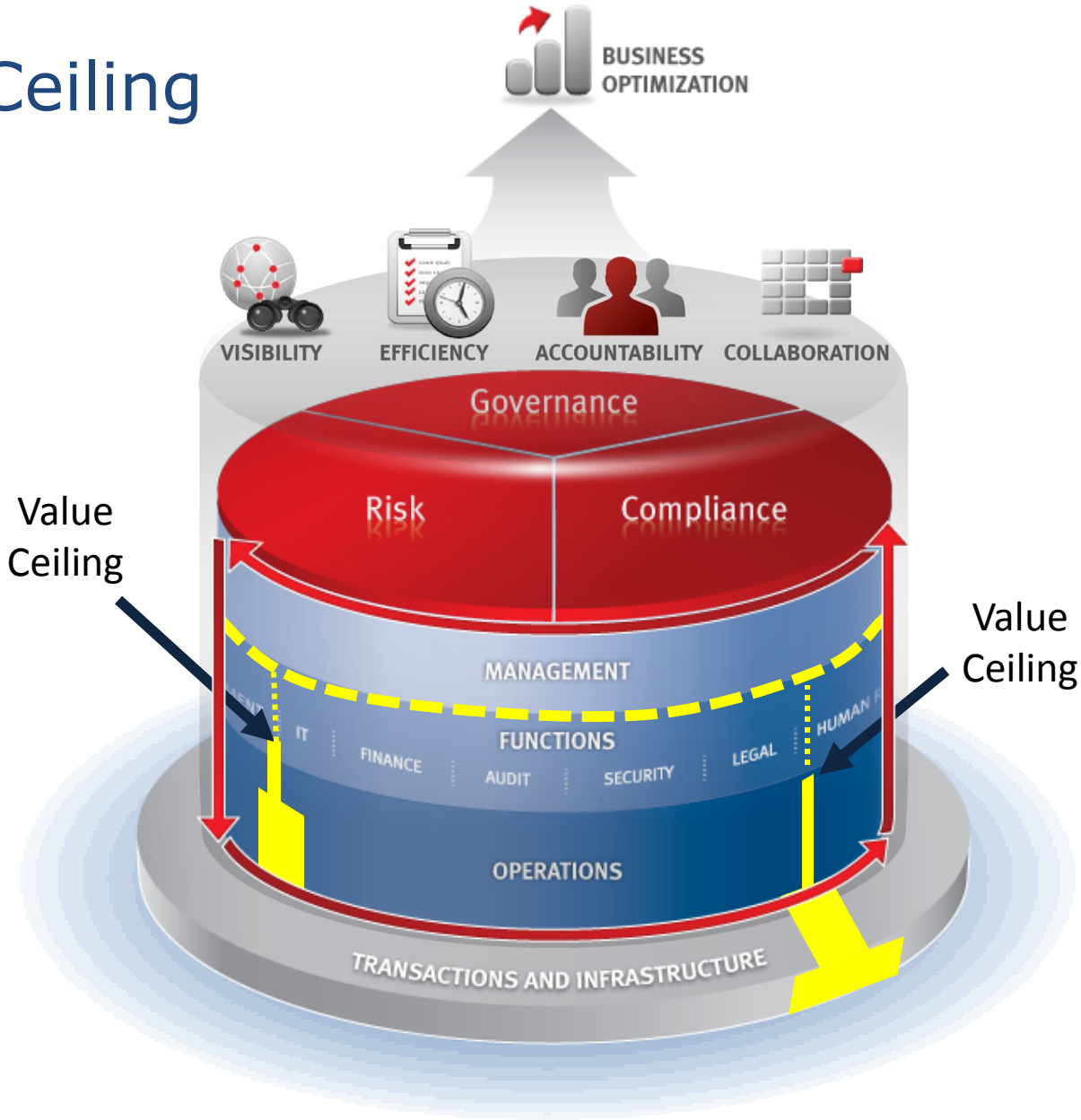
Key Processes:

- Audit Management
- Compliance Management

Key capabilities

- Control Assessments
- IT System Compliance
- Financial Reporting Compliance
- Business Process Compliance
- **Regulatory Change**
- Compliance Reporting
- Third Party Compliance

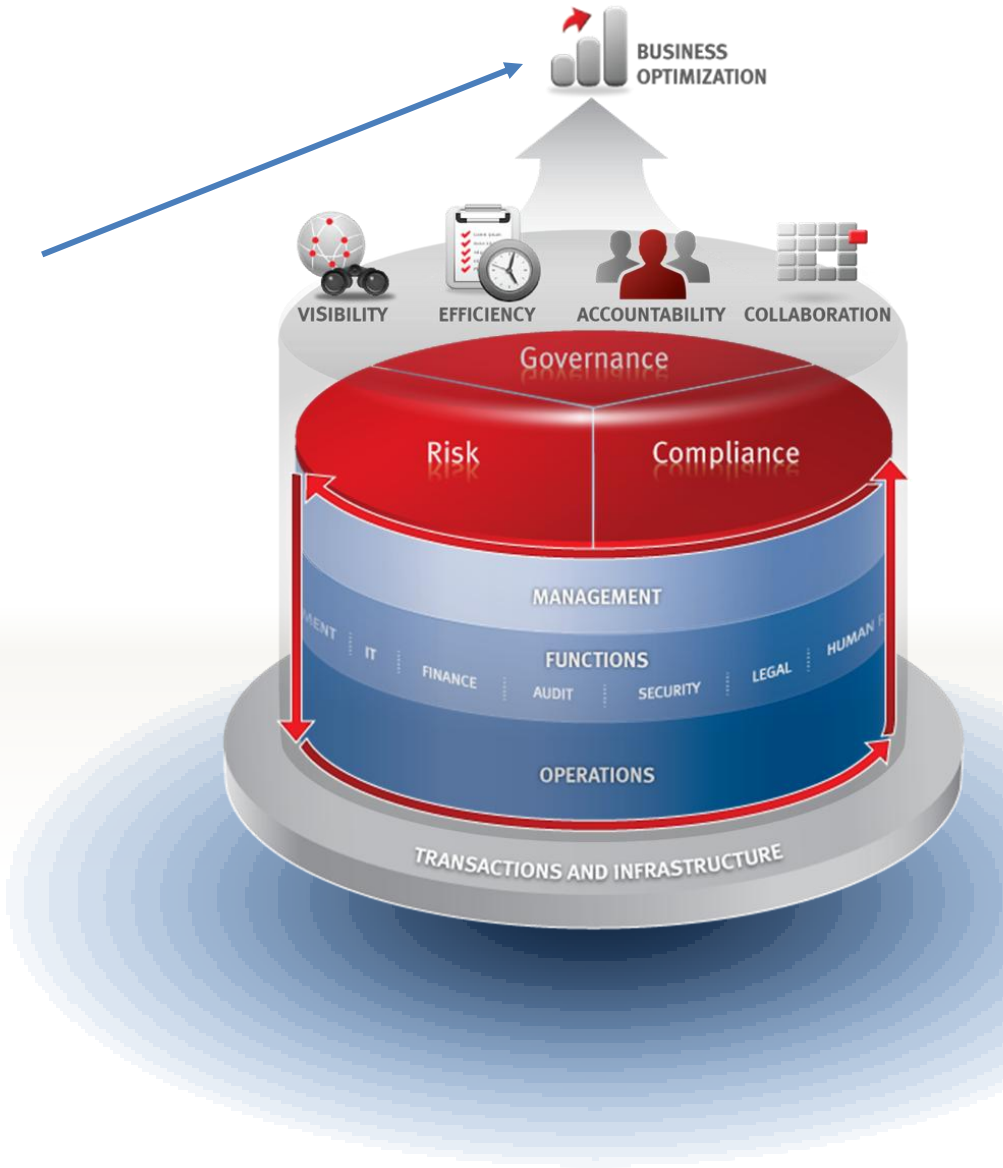
Concept: Value Ceiling



Using the RSA GRC Reference Architecture

What is the ultimate objective of the GRC effort?

What is the part of the business that the company wants to optimize?



Using the RSA GRC Reference Architecture

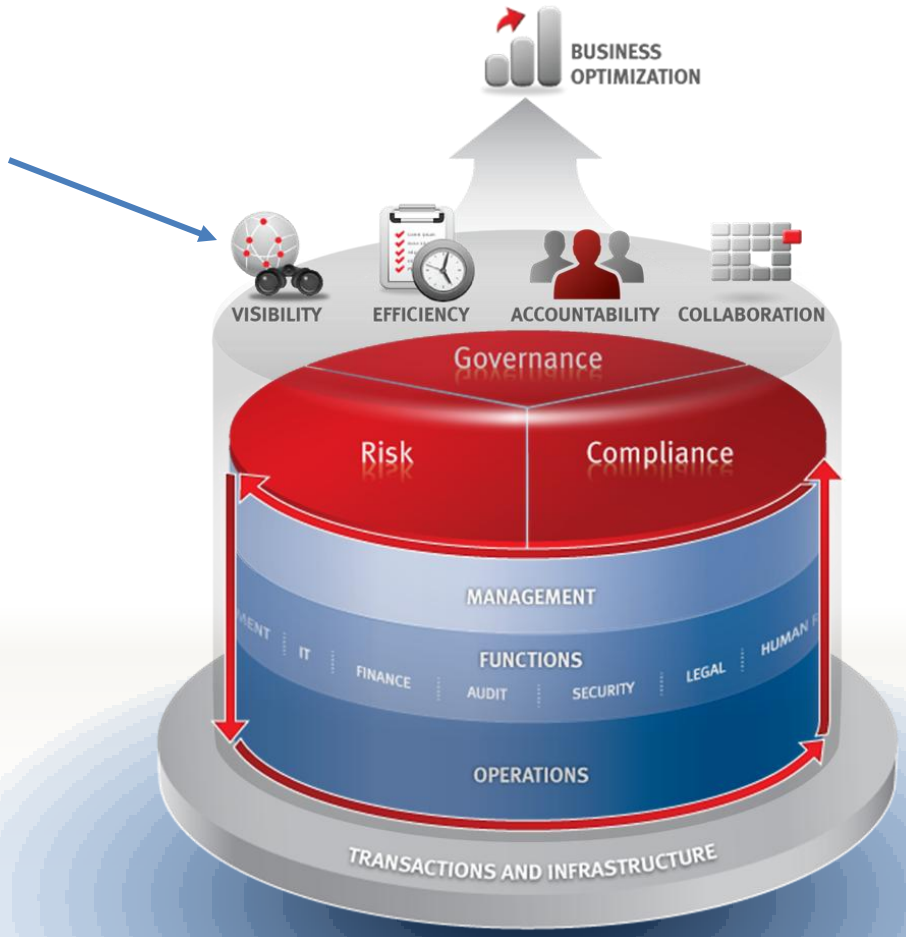
What will it take to achieve the key values?

What is the output that will provide the right visibility to make the decisions?

What processes need to be addressed? What efficiencies are targeted?

Who owns the processes? What type of accountability is being established?

How will stakeholders be engaged? What touch points between groups need to be established?



Using the RSA GRC Reference Architecture

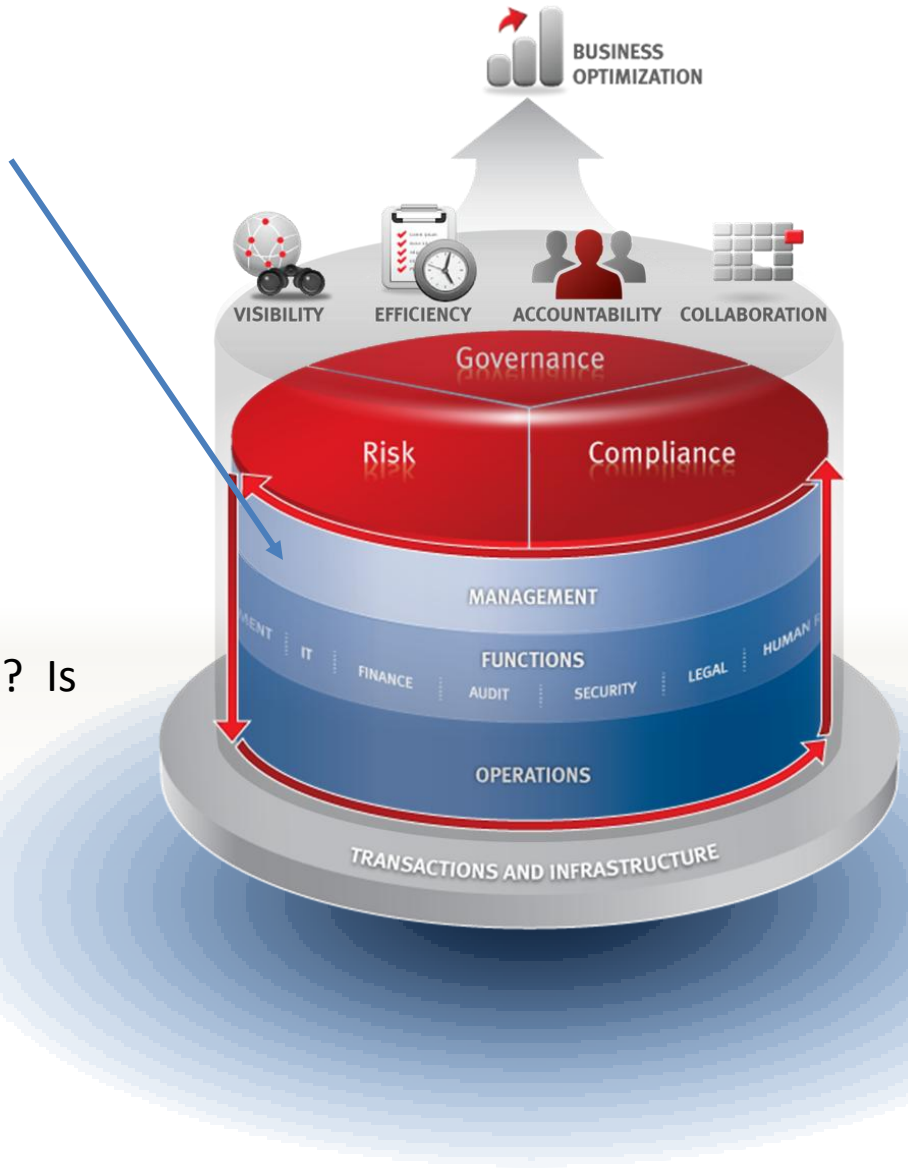
What level of management will be affected?

Who is the owner?

Who are the key stakeholders?

How is the strategy being directed?

Is there top down guidance? Is it communicated? Is it clear?



Using the RSA GRC Reference Architecture

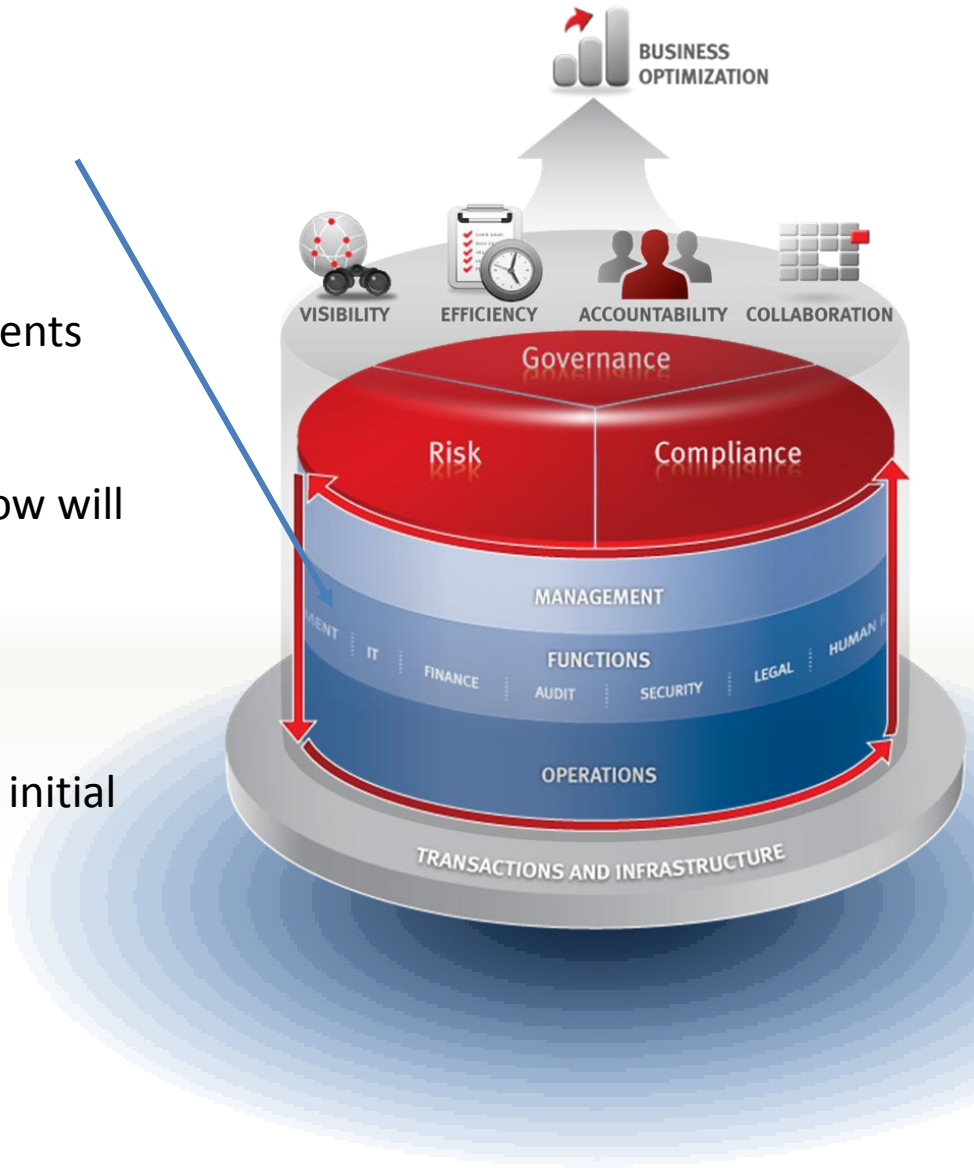
What are the Functional elements involved?

What departments or organizational components are affected?

How do the functions communicate now? How will they in the future?

What level of coordination is needed?

Is there a plan to expand or grow beyond the initial functional groups?



Using the RSA GRC Reference Architecture

What are the Operational elements involved?

What operational groups are affected?

What operational processes need to be established? Adjusted? Re-engineered?

What is the effort to sustain the operational impacts? How does the effort continue into the future?

Training, awareness, education and rollout impacts to frontline employees?

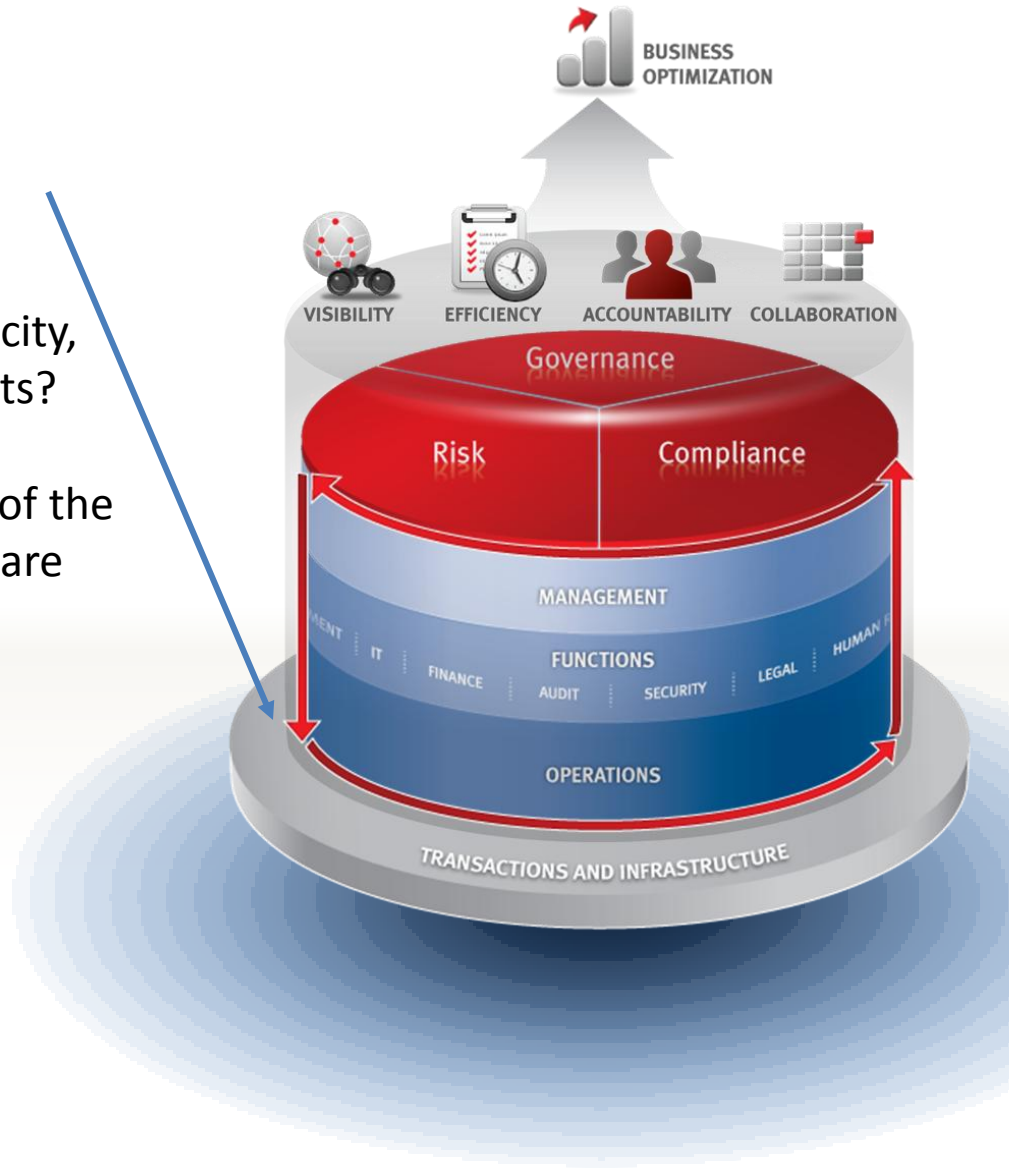
Using the RSA GRC Reference Architecture

What are Transactions and Infrastructure are relevant?

What events are impactful? What is the velocity, volume, size, scope and nature of these events?

What systems are involved? What elements of the infrastructure (facilities, IT applications, etc.) are involved?

What is the technical overhead?



Using the RSA GRC Reference Architecture

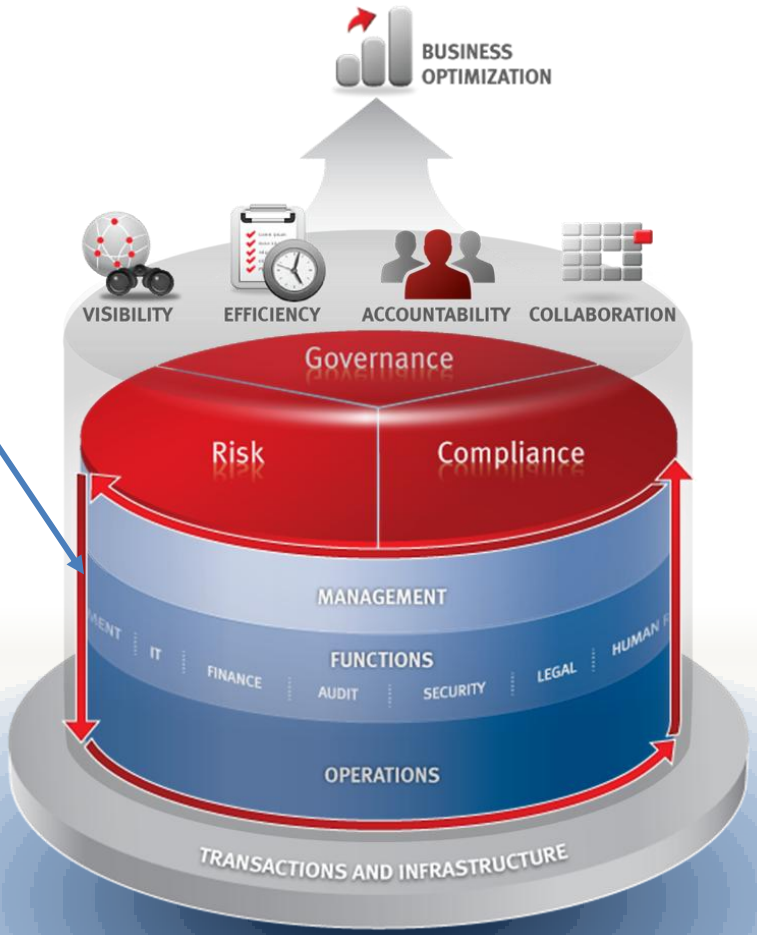
What are Feedback/Continuous Improvement needs?

How will requirements and expectations be pushed down through the stack?

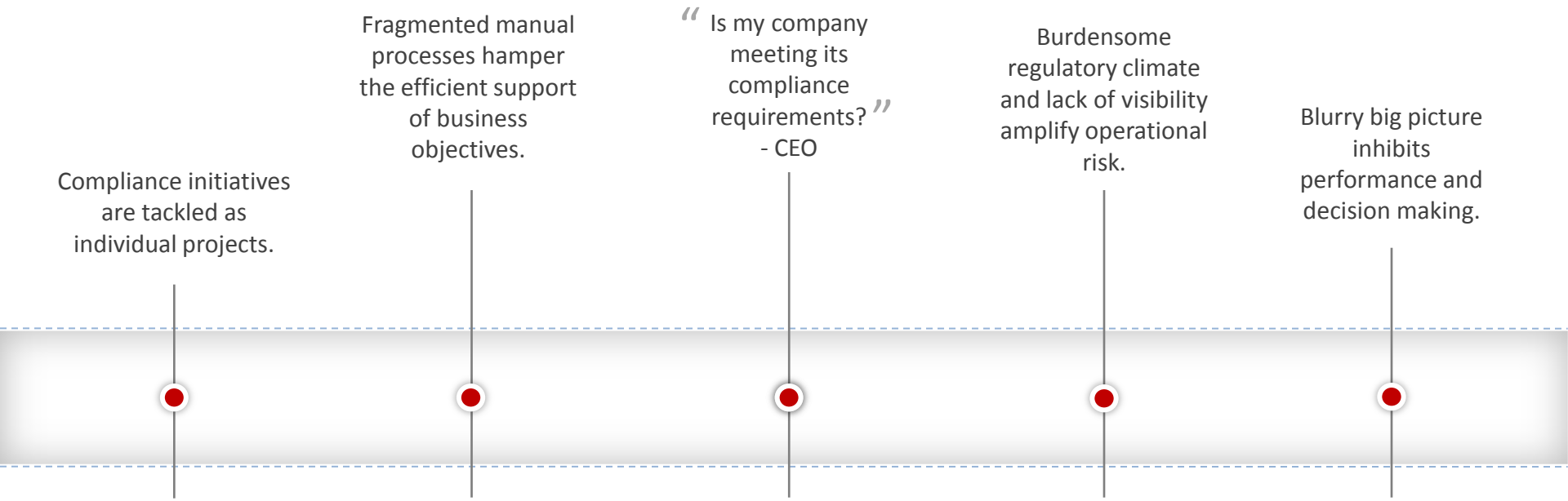
How will operations manage the transactions and infrastructure to gather the right “feedback” data?

What data is needed to be fed up the “stack” to provide to management?

How will management decide if things are operating as expected? What is the process to adjust the environment based on the feedback?



Positive Business Outcomes



Efficiency

Centralize the program to improve accuracy and eliminate wasted cycles.

Automation

Leverage technologies with intelligent workflows to prioritize work streams.

Visibility

Get the answers needed to make better, faster business decisions.

Collaboration

Integrated reviews ensure stakeholders can measure and respond to changes effectively.

Accountability

Establish governance and ownership across the policy and compliance spectrum.


trust
in the digital world