Sharing Policy Rules for IT Governance

Adrian Bowles, PhD

Program Director, Governance Risk Management & Compliance Roundtable

www.grcroundtable.org

October 2007

adrian@omg.org

adrian@cosource.net

Sharing IT Governance Policy Rules

- The OMG and GRC
- IT Governance
- Collaborative IP Development as a Business Model
- The GRID
- The GRC-RT ITG Project

Introduction

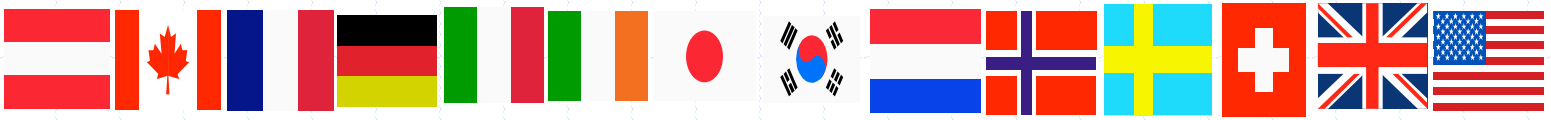
- The Object Management Group was founded in 1989. Today, with over 470 member organizations, OMG is the largest and longest standing not-for-profit, open-membership consortium developing and maintaining computer industry specifications.
- OMG members define standards with a worldwide, neutral, open, accessible and *rapid* development process that assures *freely available specifications with implementations*
- OMG members are currently developing standards in two dozen verticals including:
  - Finance, Healthcare, BMI (business modeling & integration)

OMG Specifications

OMG Relationships

Worldwide Scope

88Solutions	Credit Suisse	IDS Scheer	NASA	SAP
Adaptive	Daimler-Chrysler	IONA	NIST	Siemens
Adobe	Deere & Co.	Interactive Objects	Nokia	Sun
Alcatel	EDS	Kaiser-Permanente	Northrop	Telefonica
BAE Systems	Fujitsu	Kennedy Carter	Oracle	Thales
BEA Systems	General Dynamics	Lockheed Martin	Promia	Toshiba
Boeing	HP	MedicAlert	PrismTech	Unisys
CA	Hitachi	Mentor Graphics	Raytheon	VHA
Cisco	IBM	Motorola	Rockwell	W3C



GRC Today: Basic Findings

- Governance issues are pervasive, so identifying and exploiting common enterprise and IT governance best practices will pay increasing dividends;
- Regulatory compliance costs IT departments billions of dollars annually
- Rules are often complex, occasionally in conflict with each other, and always subject to change.
- Competitors within a market typically gain no sustainable advantage through their GRC investments, but divert capital and management resources that could be used to grow their enterprises.
- Failures can cause cascading loss of confidence within a market, so it is to every participant's advantage to collaborate and share these practices.
- GRC tools should interoperate seamlessly using open specifications for GRC data representation.

OMG's GRC Activities

- RC-SIG
  - Established 4/2005
  - Following the OMG process to develop modeling standards to represent regulations, facilitating automation of compliance tasks
  - Met throughout 2005 to identify key requirements for RC modeling
  - Currently preparing RFPs
- GRC Roundtable (GRC-RT)
  - Moderated Forums, Events, & Research
  - Global Rules Information Database (GRC-GRID)

- These programs have been supported by IBM, CA, HP, Unisys, Fair Isaac, Pegasystems, Adaptive, Lumigent, InRule and several large user organizations

GRC-Roundtable

The GRC-Roundtable will provide global GRC professionals with:

- *A Moderated Community* – Open and ongoing exchange of information is critical to achieve the goals of the GRC-RT. Electronic and in-person exchange of ideas and experiences is critical, so the GRC-RT provides continuity through online forums complemented by live events held around the world.
- *A Voice* – The GRC-RT is uniquely positioned as a unifying force in the GRC market. It acts as a GRC IP integrator, bringing together the best concepts, mappings, controls and frameworks while exploring the needs and concerns of its members. The GRC-RT will produce and disseminate research findings in the form of webinars, white papers, and events to educate and shape public and government opinion based on the experiences of its members.
- *Resources* - The GRC-RT is developing the ***Global Rules Information Database (GRC-GRID)*** – an open database of GRC rules, regulations, standards, and government guidance documents, as well as a survey of the regulatory climate around the world.

GRC-Roundtable

The GRC-Roundtable will:

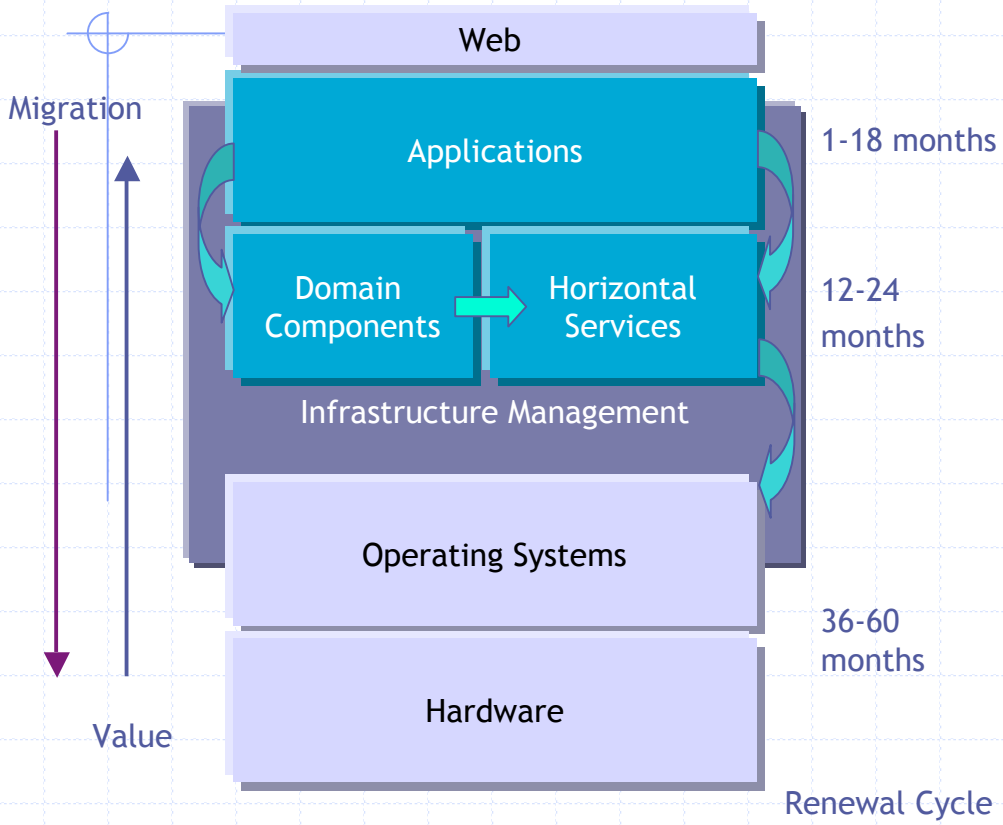
- Support leading developers of GRC frameworks and information, including ISACA, IT Governance Institute, IT Compliance Institute, etc. and provide a forum to encourage and enable interoperability of their IP.
- Support the OMG's efforts to develop and disseminate specifications for GRC data representation and capture.
- Collaborate with regulators and their affiliates, such as the SEC, PCAOB and National Archives and Records Administration, to encourage the publication of proposed and enacted rules in standard formats to support automated analysis, interpretation, and compliance wherever feasible.
- Facilitate the community-oriented development and distribution of common rules for domains of interest to members.
  - The first such set is for IT Governance

What is IT Governance *and why should I care?*

IT Governance (ITG) is

- An emerging discipline
  - focused on managing and improving the delivery of IT through improved alignment with business goals and strategy, value delivery and risk management. ITG supports IT through all aspects of business (from innovation through growth and operations).
- A critical business issue
  - as IT failures rooted in process errors are too common and the resulting loss of revenue, reputation, and opportunity are unacceptable.
- Part of a good corporate governance structure
  - used to help ensure that IT delivers *what* is expected, *when* it is expected.
- An opportunity for business differentiation
  - through delivery of superior IT services.

ITG is Critical Because IT-Based Competitive Advantage is Fleeting

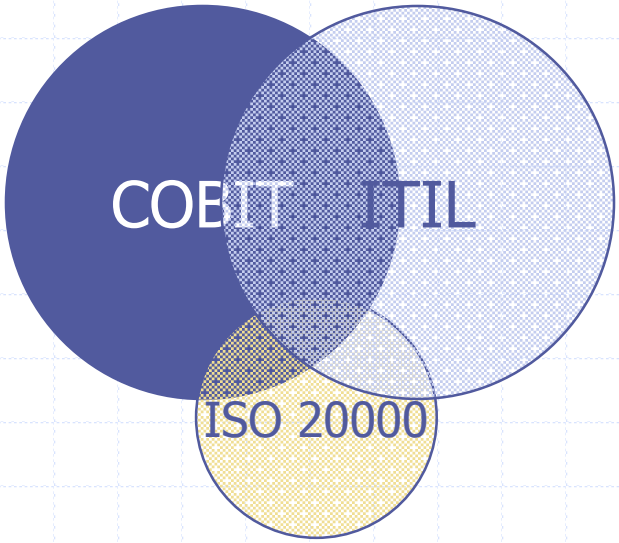


- Applications can't differentiate indefinitely.
- Timely delivery of new IT projects and services is critical to sustained growth and profitability.
- ITG offers benefits throughout the lifecycle from concept to code and operations.

Leading Frameworks: Converging IP from Competing Organizations

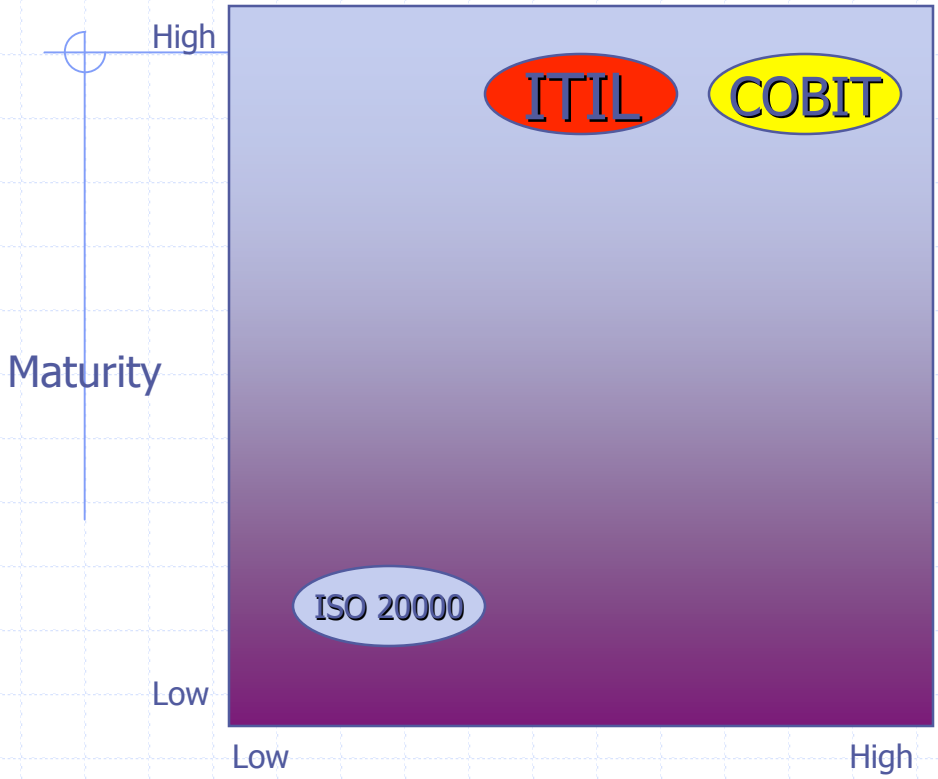
Framework	Source	Notes
ITIL (IT Infrastructure Library)	Office of Government Commerce (OGC) UK	OGC is an organization whose mission is to generate revenue for the UK Treasury via book and online access sales and accreditation revenue (through third parties TSO and APMG).
COBIT (Control OBjectives for IT)	IT Governance Institute (Affiliate of ISACA)	Professional association whose mission is to provide benefit to members. IP developed by membership and ITGI staff. Focused on management controls, management practices, governance, closely aligned with Sarbanes Oxley requirements. Member benefits to advance ISACA/ITGI organization value.
ISO 20000 (IT Service Management Standard)	ISO IEC – international standards body – members are national standards bodies.	International standard. Overlapping management system and certification standard with 9001 – some confusion in standards as a result. There is a related for-profit certification scheme. Certification is not part of the standard.

Convergence Trends & Issues



- Areas of overlap will continue to expand as individual frameworks evolve.
- Complete convergence won't happen.
- Although mappings/cross references between the frameworks are becoming available, it is left as an exercise for the end-user to put it all together.
- It is in the best interest of the framework developers to get users to adopt everything from their framework, and add differentiated practices from others as necessary - this is not necessarily in the best interest of the user.
- Best approach will be to adopt and integrate policies representing the best/most relevant practices from each, but avoid lock-in to any one of them.

Frameworks are Business Focused

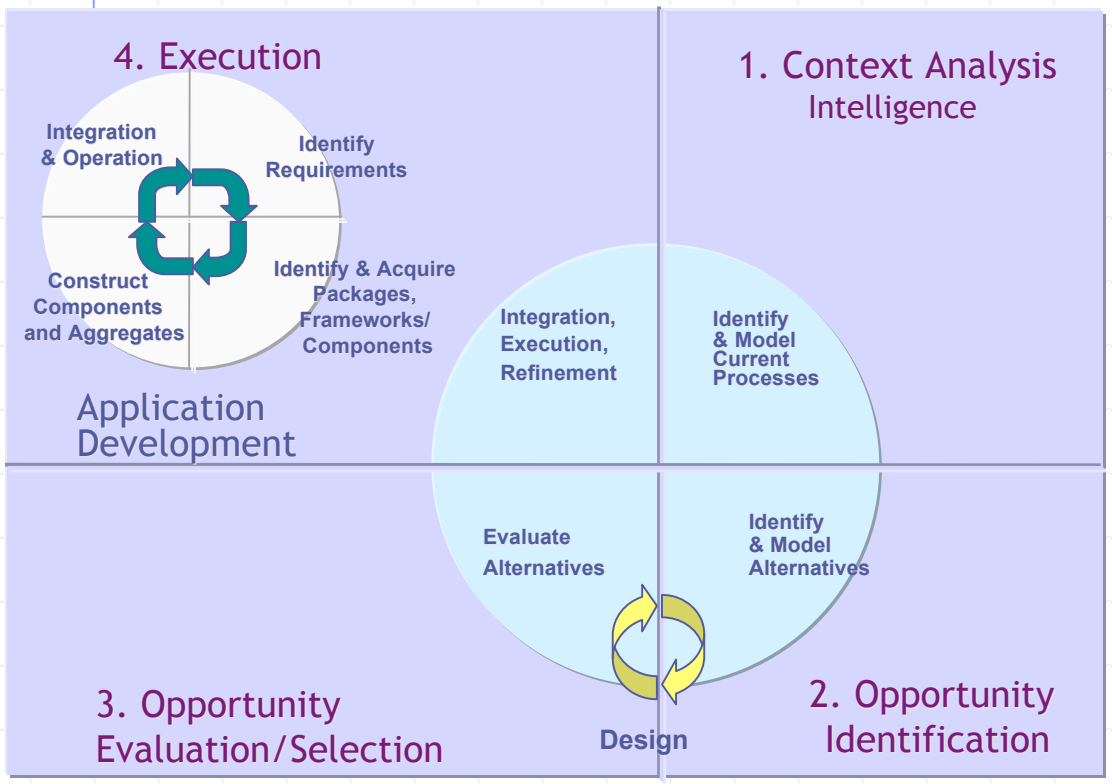


These frameworks address key business objectives of improving service delivery and operations, but the leaders come from different backgrounds.

- COBIT reflects business concerns in IT (Driven largely by governance regulations like Sarbanes Oxley Act)
- ITIL & ISO 20000 reflect IT concerns in business (Need to overcome traditional IT process weaknesses and lack of predictable results)

- All are currently being updated
- All are becoming more business-focused
  - As IT becomes more integrated into business processes
  - As increasing regulatory constraints impinge on IT management and operations

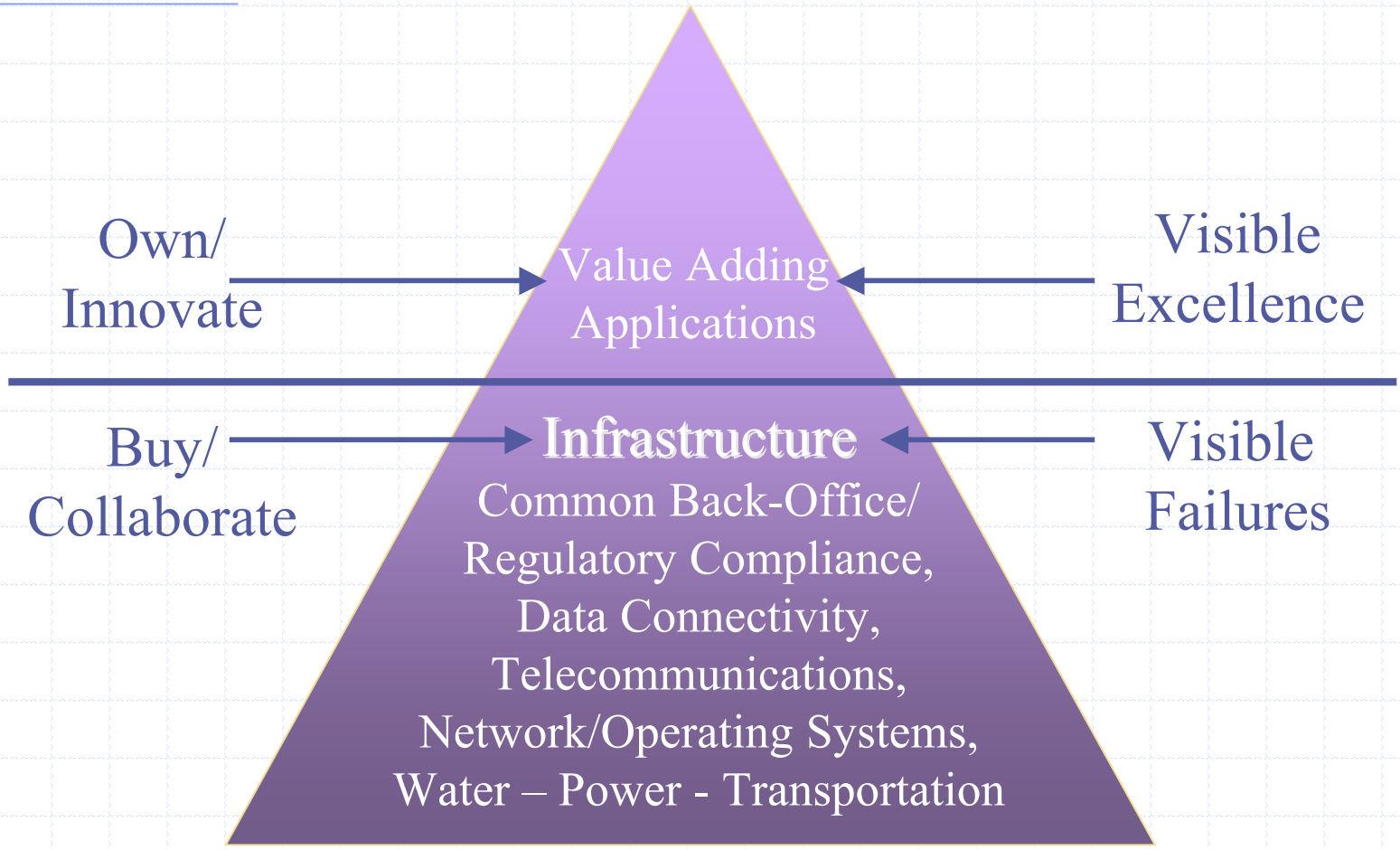
ITG Has a Role Throughout the BUSINESS Lifecycle



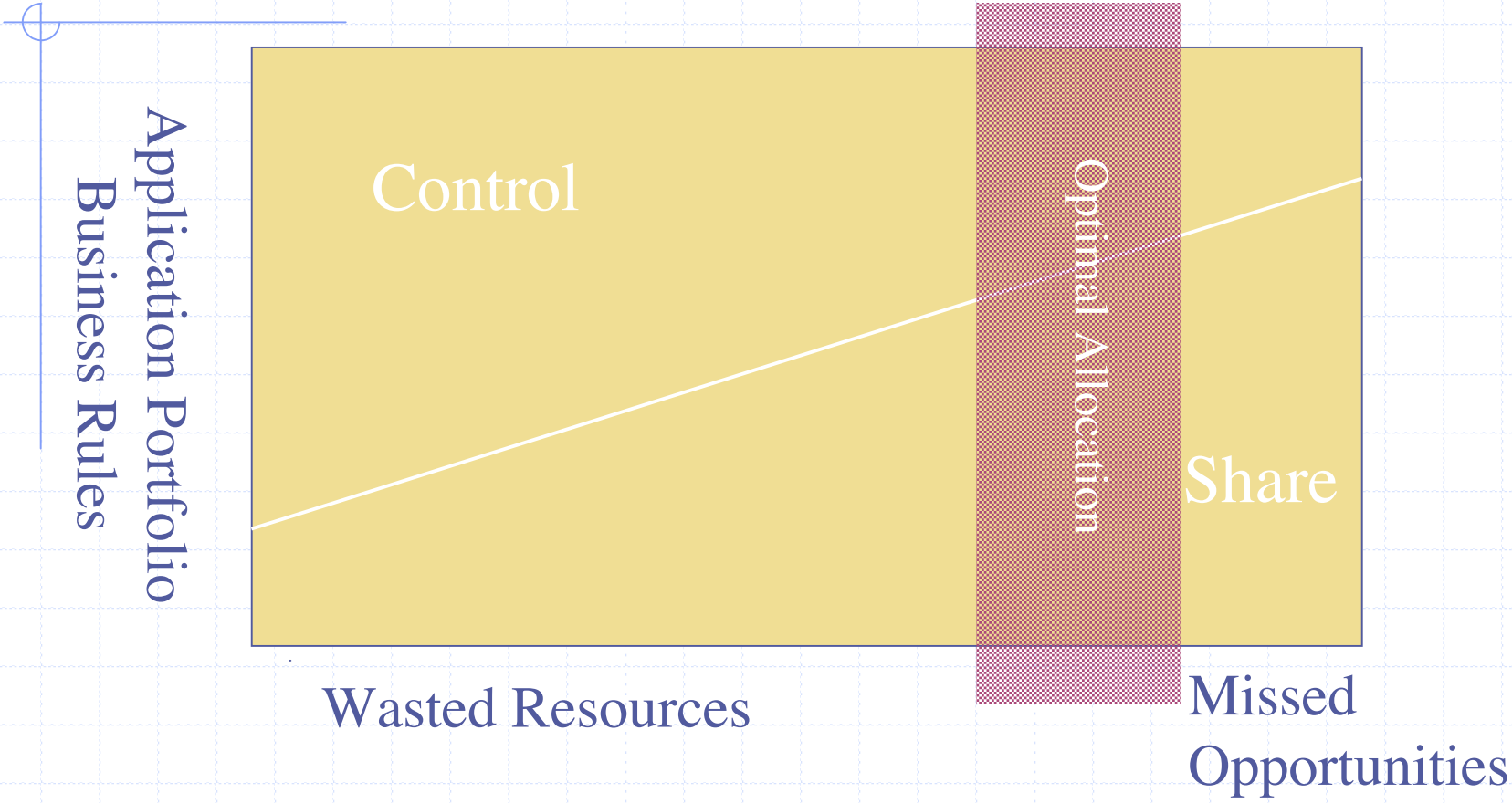
- Traditionally, IT has been seen in a supporting role ("aligned" with business objectives).
- These frameworks were developed to map to the Execution Quadrant in this Business Lifecycle model.
- Going forward, IT must be integrated into the business lifecycle, with services that support all phases of business-value delivery.

The Business Lifecycle: From Vision to Value

Focus Where Customers Notice

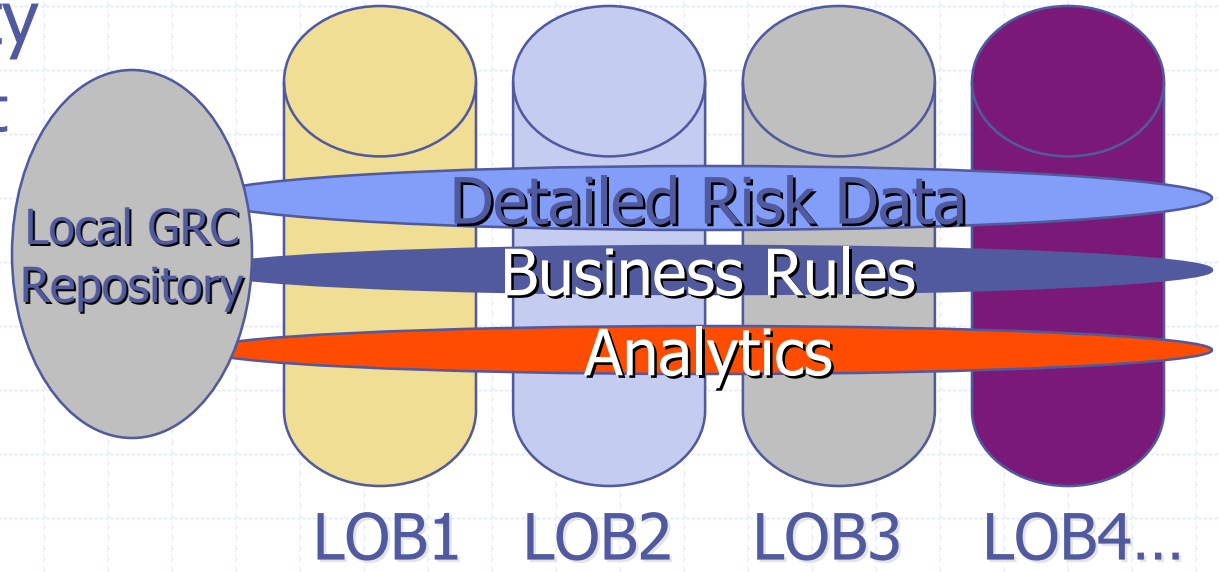


Control vs Share Strategy

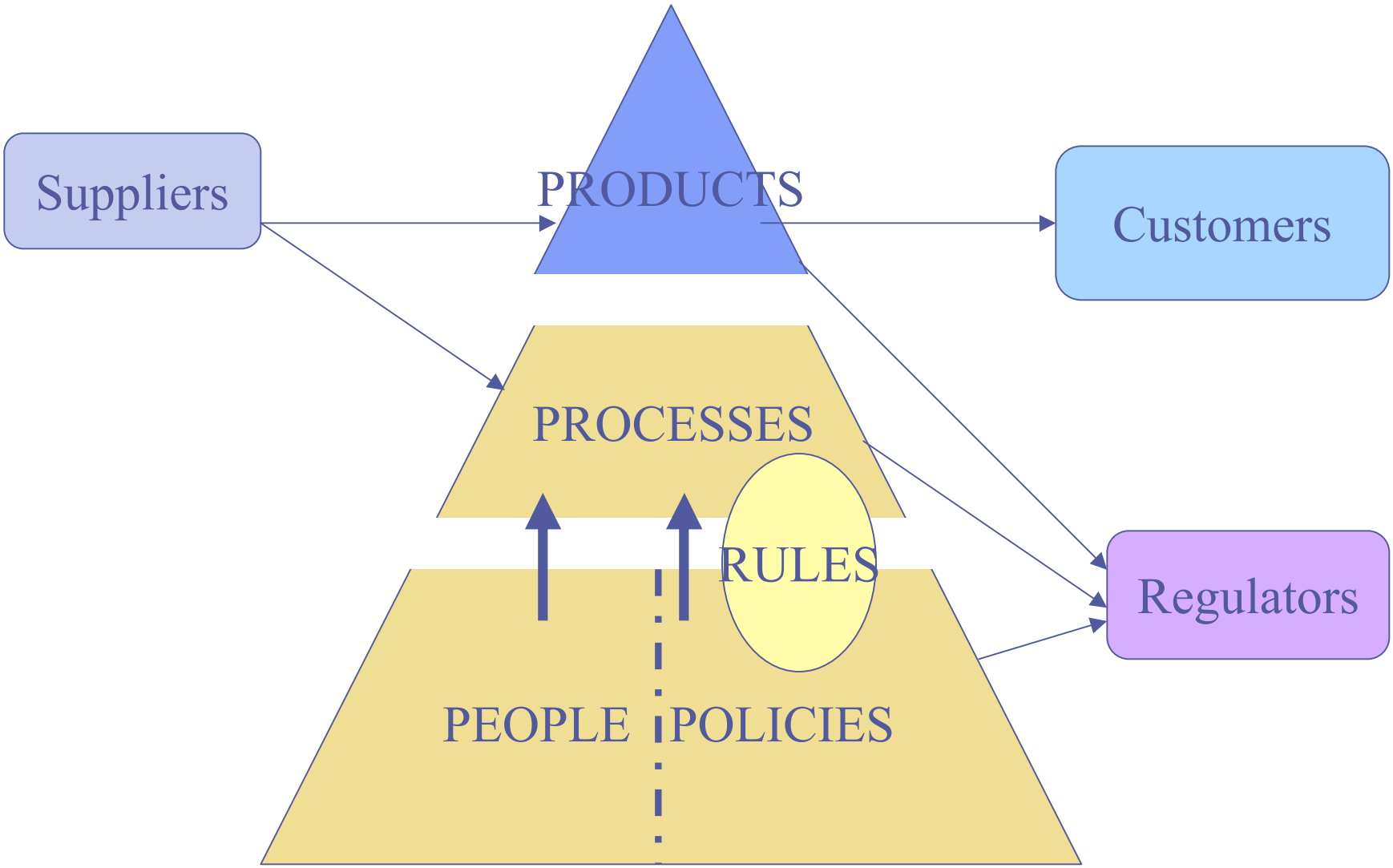


The Great Roll-Up

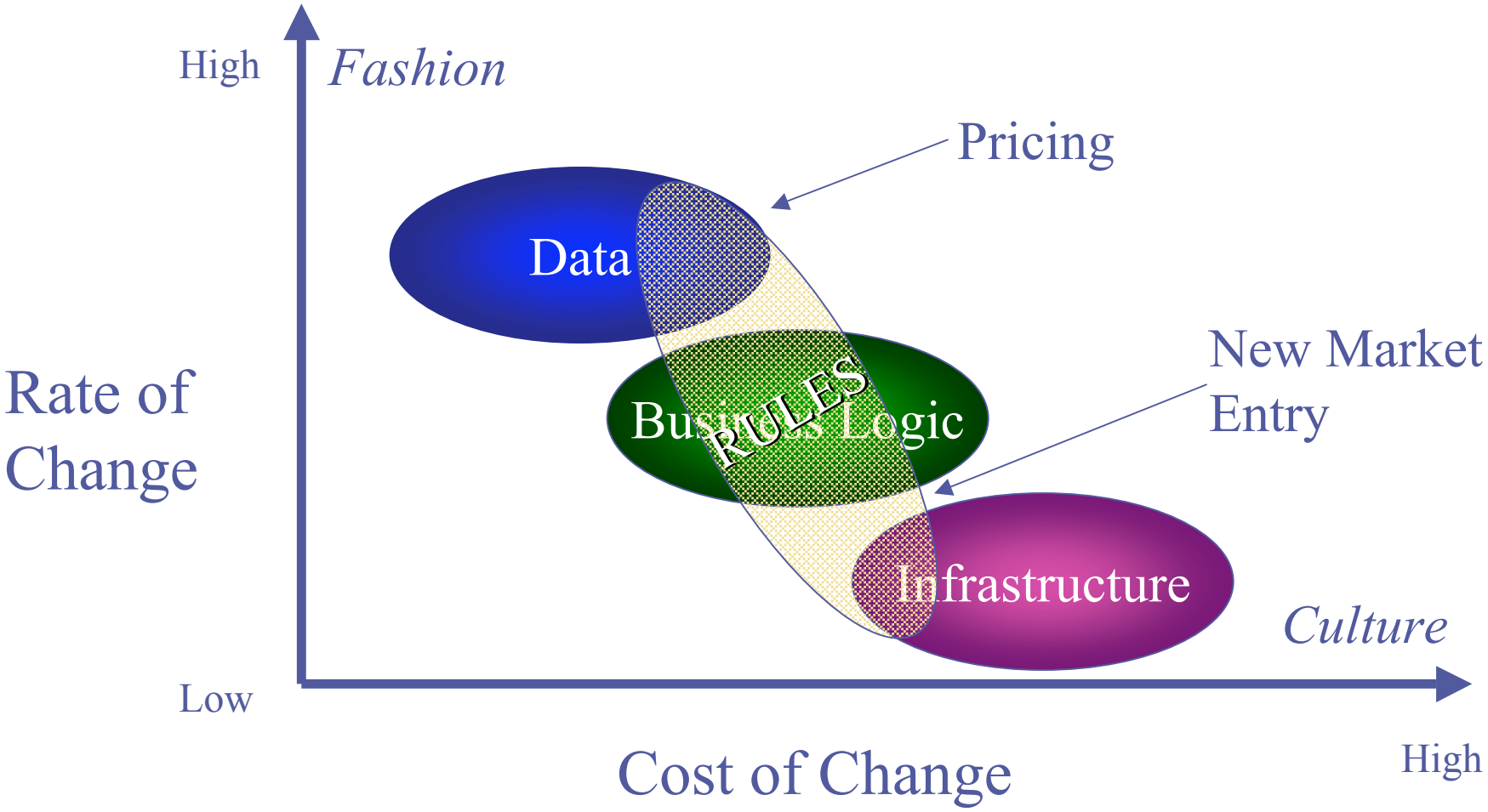
- Aggregation: Who has the big picture Vs who needs it?
- Issues
  - Data quality
    - Consistent
    - Current
    - Complete



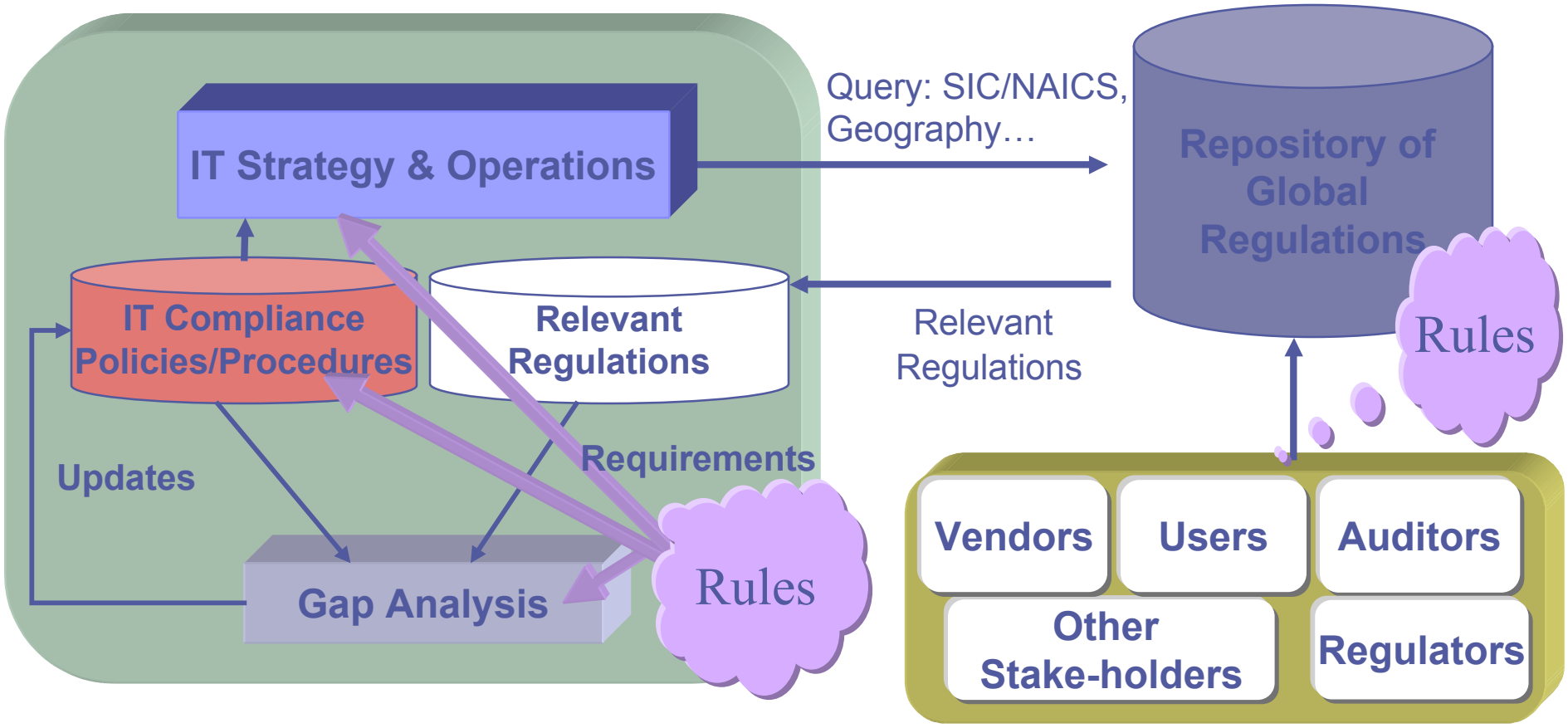
Business Runs on Rules



Characteristics of Change



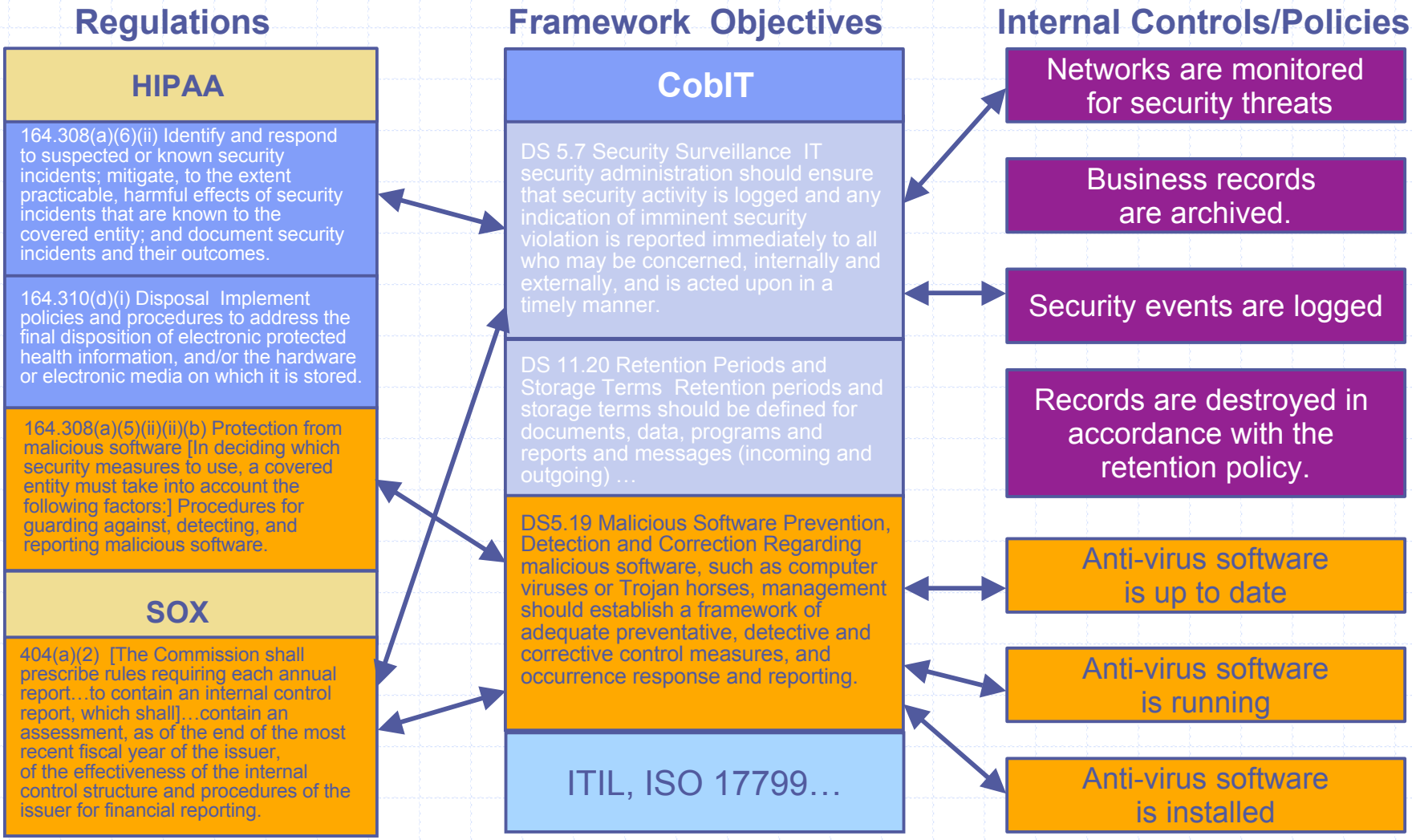
Automating GRC & IT Governance



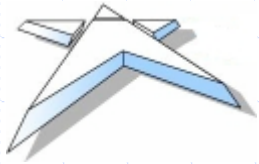
Goal: Automated Detection of New Regulatory Requirements and Rule-Based Generation of Policies

OBJECT MANAGEMENT GROUP

Capturing Complex Mapping Relationships



The Design Was Collaborative...



Business Semantics Ltd

Implementation and Operations are Collaborative, Too.

IBM

US NATIONAL ARCHIVES

inrule TECHNOLOGY

LUMIGENT

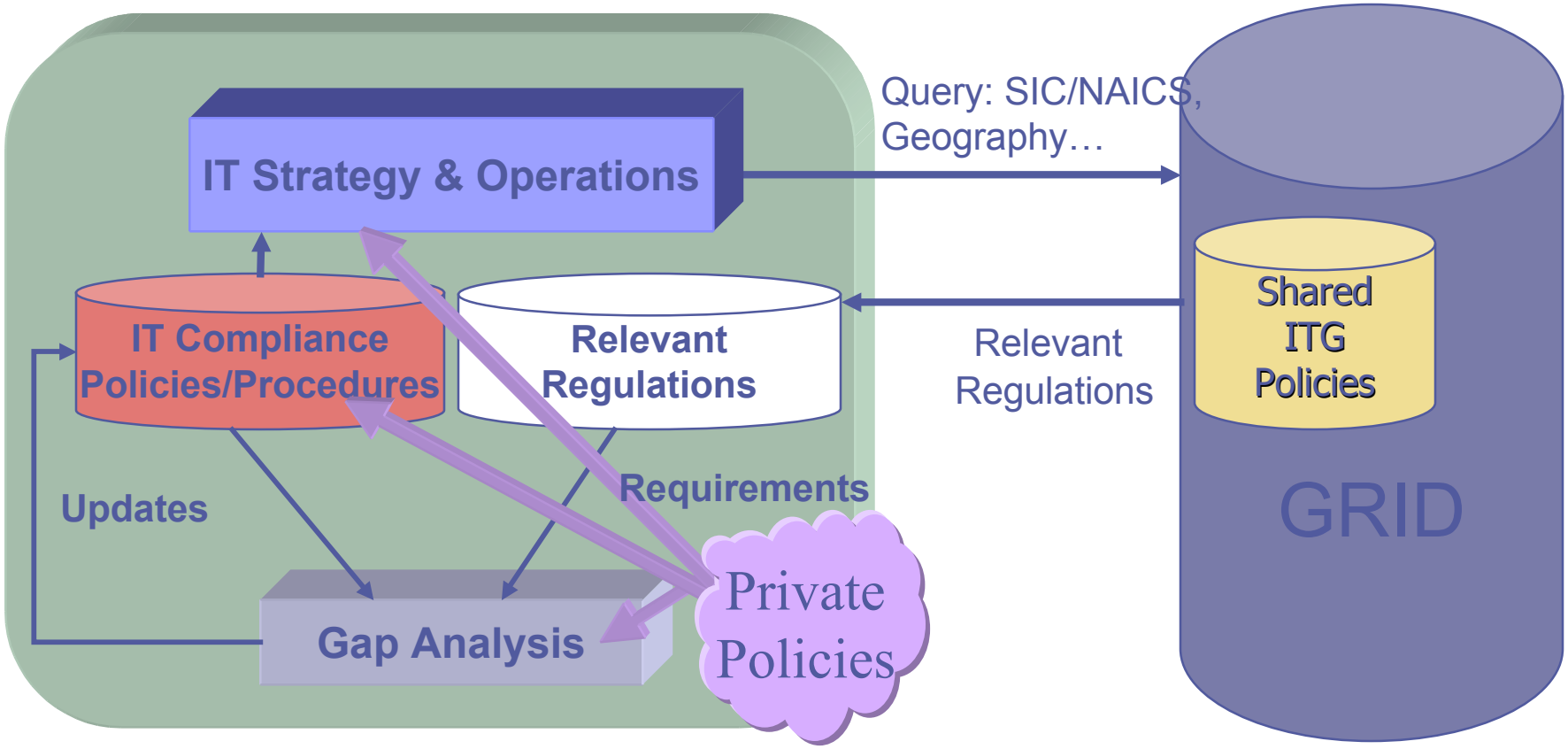
XBRL .ORG

Already received compliance and privacy data on over 100 countries from individuals, top tier banks and brokerage firms.

The GRC-RT ITG Project

- Goals - Identify/build a common set of ITG Policies with broad applicability, and make them available via the GRID
  - Participation is open to all GRC-RT members
  - Cultural Challenges - Some firms exhibit NIH syndrome
  - Technical Challenges
  - Benefits
    - Reduced Cost
    - Reduced Risk
    - Better Coverage and Currency

Supporting Shared IT Governance Practices



The GRC-RT ITG Project

Status

- New Initiative
- Forum to be launched in December 2007
- at www.grcroundtable.org
- Kickoff meeting to be held in Q1 2008
- Ready to share IP with individual firms and associations now.
- First step will be to identify all relevant frameworks and existing overlaps and mappings.

Sharing Policy Rules for IT Governance

Adrian Bowles, PhD

Program Director, Governance Risk Management & Compliance Roundtable

October 2007