

The Global Rules Information Database

developed for the
**Governance, Risk Management
& Compliance Roundtable**

**Adrian Bowles, Ph.D.
Said Tabet, Ph.D.**

Object Management Group
<http://www.omg.org>



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



THE *Open* GROUP



OBJECT MANAGEMENT GROUP

Copyright © 2007 by OMG. All Rights Reserved.

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

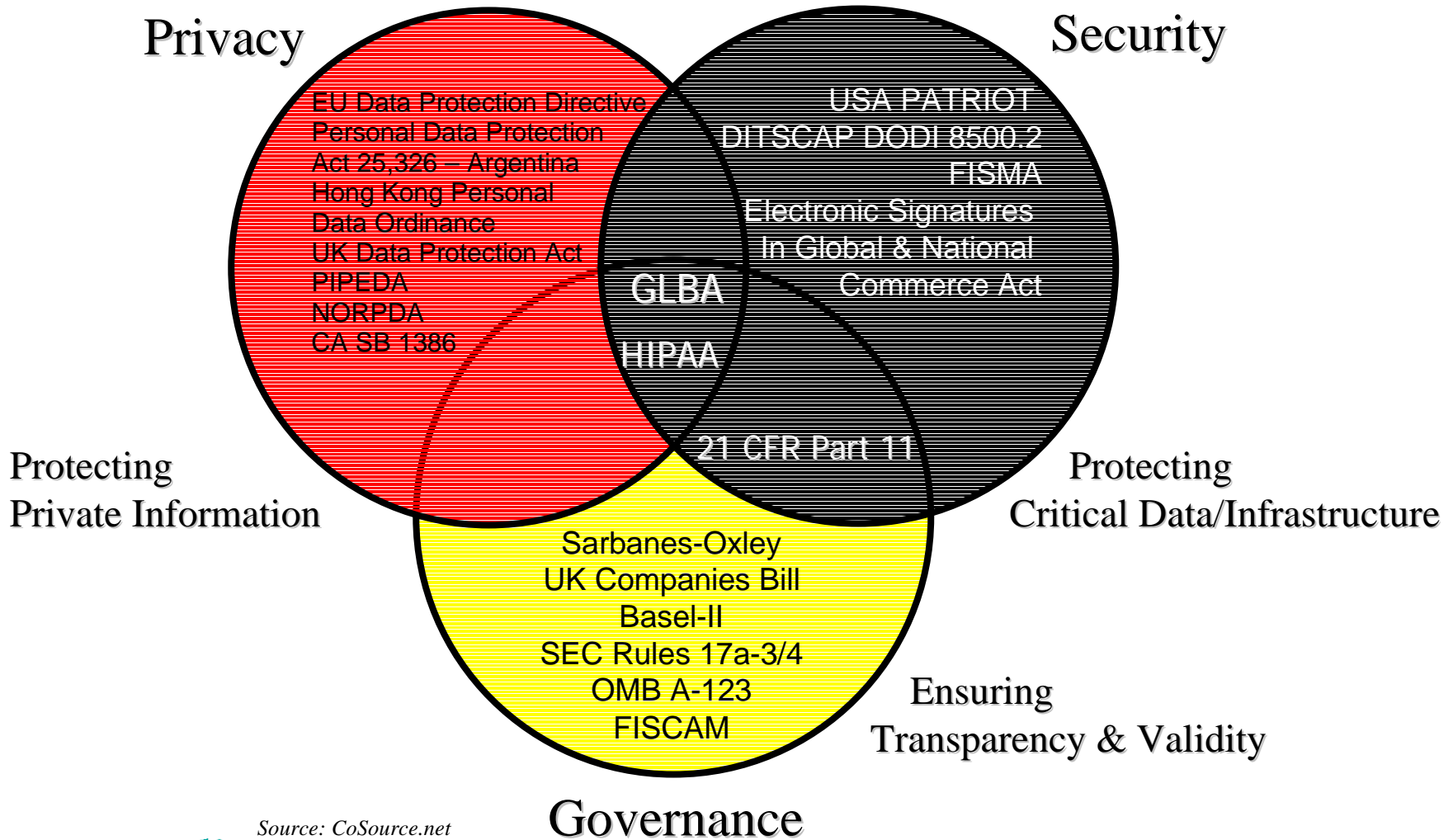


The OMG and Regulatory Compliance

- OMG Members - mostly global firms - were struggling with regulatory compliance costs and complexities
- OMG reviewed available resources, and determined that a lack of standards for modeling regulations was hindering development of better tools to automate common compliance tasks
- The OMG launched initiatives to address these issues in April 2005



Overlapping Intents & Requirements



Source: CoSource.net



GRC Today: Basic Findings

- Governance issues are becoming pervasive, so identifying and exploiting common enterprise and IT governance best practices will pay increasing dividends;
- Enterprise risk management is emerging as a cross-functional discipline, but progress is hampered by the lack of relevant standards and interoperable tools;
- 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 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, OCEG, 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.



GRC-RT *Participants* are entitled to:

Administrative Benefits

- Attend and vote at all general and special meetings of the Membership.
- Nominate one representative to serve on the GRC-RT Steering Committee, subject to election. The Steering Committee is responsible for the strategic direction of the GRC-RT.
- Propose initiatives to be acted upon by the GRC-RT Steering Committee; and
- Such other benefits, rights and privileges as the GRC-RT Steering Committee may from time to time approve.

Collaboration/IP Benefits

- Attend quarterly general meetings hosted by the GRC-RT, and up to 6 regional meetings annually, hosted by members upon request, and special meetings as called by GRC-RT management.
- Participate in the GRC-RT general forum, topic forums, mailing lists, and other collaborative media provided by the GRC-RT.
- GRC-RT staff will moderate the general forum, while Participants may initiate and moderate topical forums.
- Obtain early access to IP contributed by other GRC-RT members.
- Contribute and vet data for the GRC-GRID. Influence the GRC-GRID development priorities.
- Poll the Membership on GRC issues provided the posting member is identified and the results of the poll are shared with the community. Aggregated results may be synthesized in reports prepared by the GRC-RT management for external distribution.

Promotional Benefits

- Place a link to such Member's Web site on the GRC-RT Web site.
- Display the GRC-RT logo on Participant's Web site to indicate membership in the GRC-RT.



GRC-RT *Sponsors* are entitled to:

All the Benefits of *Participant Membership*, and

Enhanced GRC-GRID Access

- Worldwide, unrestricted access to the GRC-GRID. (e.g., ability to download and directly interface with local copy of database or public copy).
- Seat on the GRC-GRID Advisory Board, which provides strategic input to the development team and prioritizes new features and functions. Sponsor's staff may help with GRC-GRID development, to prepare them to develop internal systems that use GRC-GRID data.

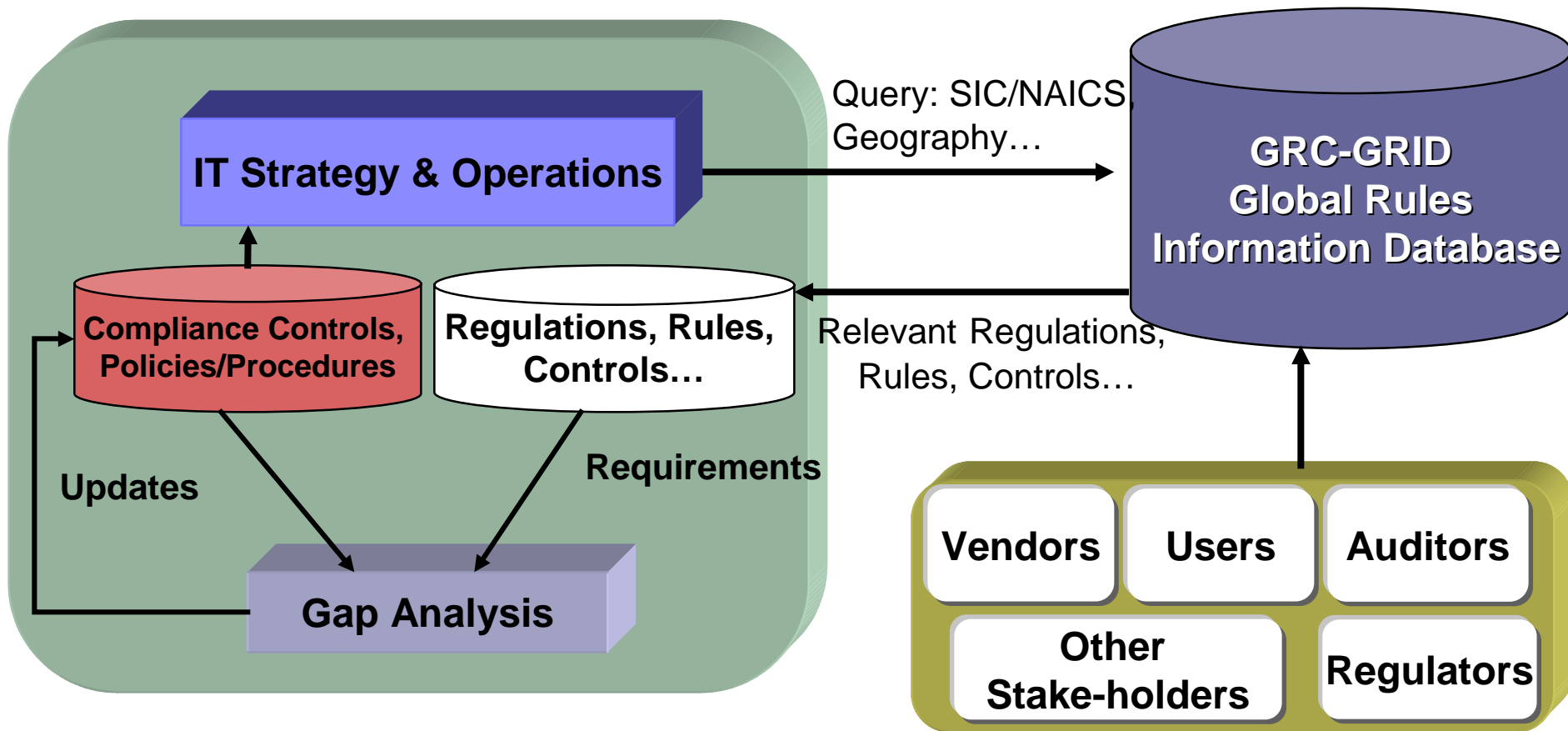
Research & Marketing Opportunities

- Sponsorship logo on the GRC-GRID.
- Post their own webinars, white papers and additional IP to the GRC-RT general forum for feedback, and to a public forum for PR
- Identification as a GRC-RT Sponsor on all GRC-RT collateral, with logo placement.
- Identification as a GRC-RT Sponsor at all GRC-RT events, with logo placement on banners and event collateral.
- Demonstration space at all GRC-RT events.
- Exposure for Sponsor as GRC thought-leader in GRC-RT webinars, events, PR campaign.
- Webinars and events will be produced and co-marketed by GRC-RT and its Sponsors. Featured will be individual presentations by invited speakers, interviews with GRC-RT management and advisors, as well as panel discussions. Sponsorships will feature the sponsor's logo and name on the webinar itself and on all promotional materials, as well as post-meeting materials. The webinars will be available on-demand on the GRC-RT web site.

Founding Sponsor: A limited number of Founding Sponsorships are available. For details of this program, please contact Frank Yacano frank@omg.org 1-781-444-0404 X101



Automating Regulatory Compliance



GRC-GRID Goals and Objectives

- Improve the ability of **enterprises** to:
 - Effectively comply and demonstrate compliance with relevant regulations
 - Reduce the time, and initial and on-going costs of complying with regulations
- Improve the ability of **vendors** of IT based products and services to develop offerings that:
 - comply with regulations, or that
 - enable the planning, implementation and control of processes and rules to comply with regulations



GRC-GRID Goals and Objectives *(continued...)*

- Improve the ability of **regulators** to formulate regulations that capitalize on best practices and standards for complying with regulations
- Improve the ability of **auditors** and other service providers to assist enterprises to ensure regulatory compliance by applying best practices and standards



Automated Compliance Support Roadmap

1. Capture and Catalog the Requirements

Catalogs are the First Step

Regulations

HIPAA

164.308(a)(6)(ii) Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.

164.310(d)(i) Disposal Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.

164.308(a)(5)(ii)(i)(b) Protection from malicious software [In deciding which security measures to use, a covered entity must take into account the following factors:] Procedures for guarding against, detecting, and reporting malicious software.

SOX

404(a)(2) [The Commission shall prescribe rules requiring each annual report...to contain an internal control report, which shall]...contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.

Framework Objectives

CobIT

DS 5.7 Security Surveillance IT security administration should ensure that security activity is logged and any indication of imminent security violation is reported immediately to all who may be concerned, internally and externally, and is acted upon in a timely manner.

DS 11.20 Retention Periods and Storage Terms Retention periods and storage terms should be defined for documents, data, programs and reports and messages (incoming and outgoing) ...

DS5.19 Malicious Software Prevention, Detection and Correction Regarding malicious software, such as computer viruses or Trojan horses, management should establish a framework of adequate preventative, detective and corrective control measures, and occurrence response and reporting.

ITIL, ISO 17799...

Internal Controls

Anti-virus software is up to date

Anti-virus software is running

Anti-virus software is installed

Networks are monitored for security threats

Business records are archived.

Security events are logged

Records are destroyed in accordance with the retention policy.

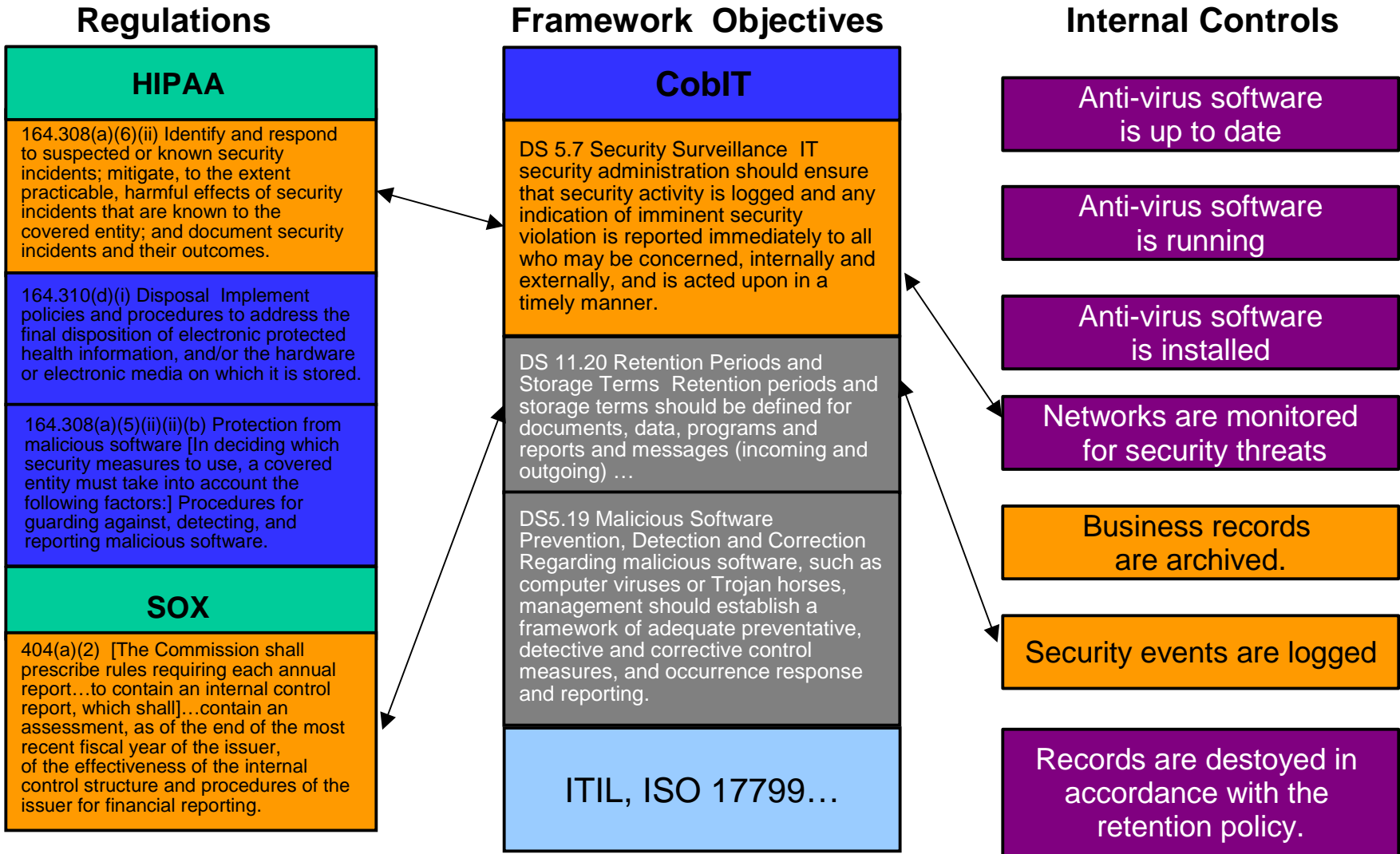


Automated Compliance Support Roadmap

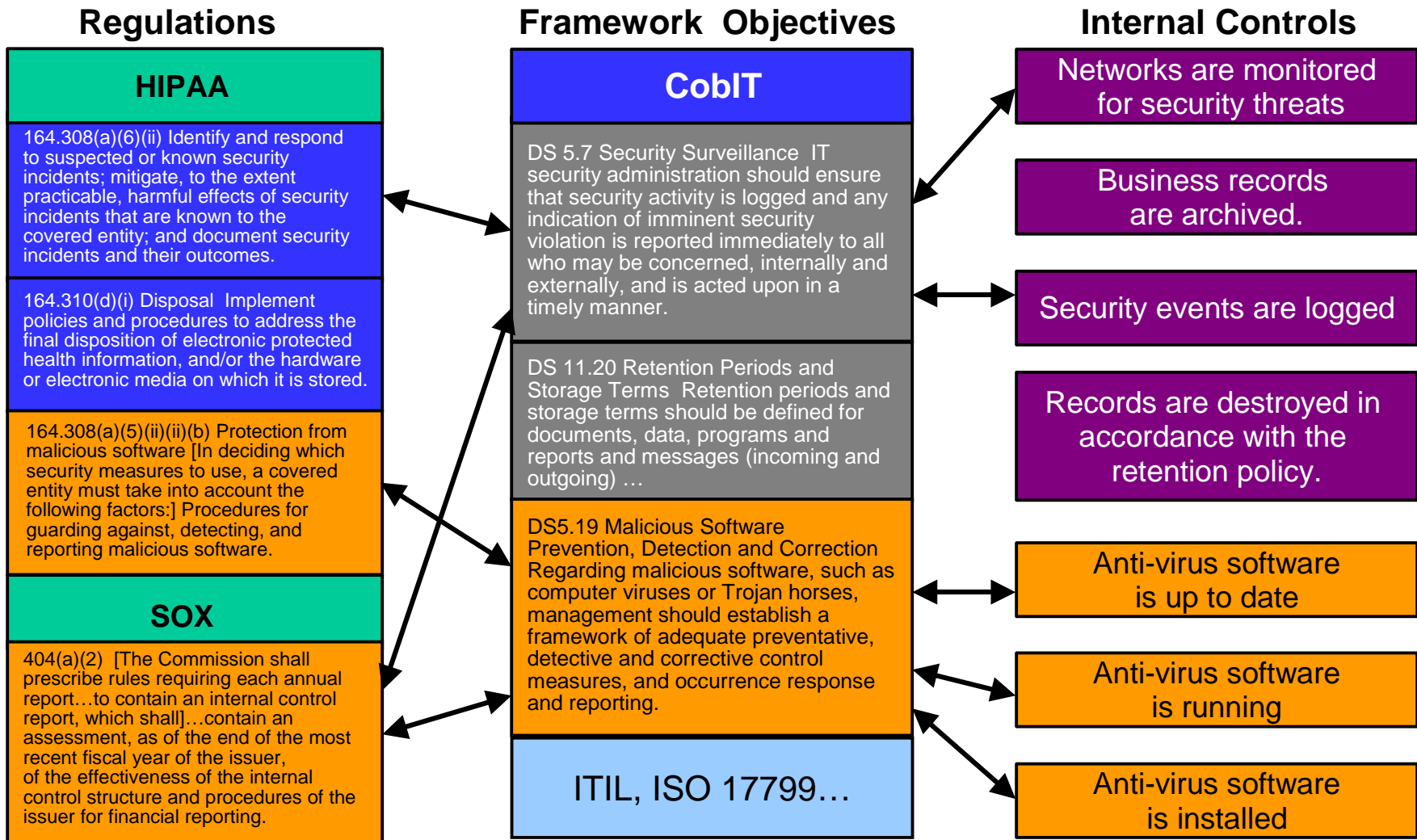
1. Capture and Catalog the Requirements
2. Capture the interdependencies between regulatory requirements and indicated IT controls (COBIT, ITIL...)

The C-GRID will provide a dynamic mapping that allows IT management to ensure that regulatory requirements are met, and that the impact of changes to controls are predictable

Bi-Directional Mapping is Critical



Capturing Complex Mapping Relationships



Automated Compliance Support Roadmap

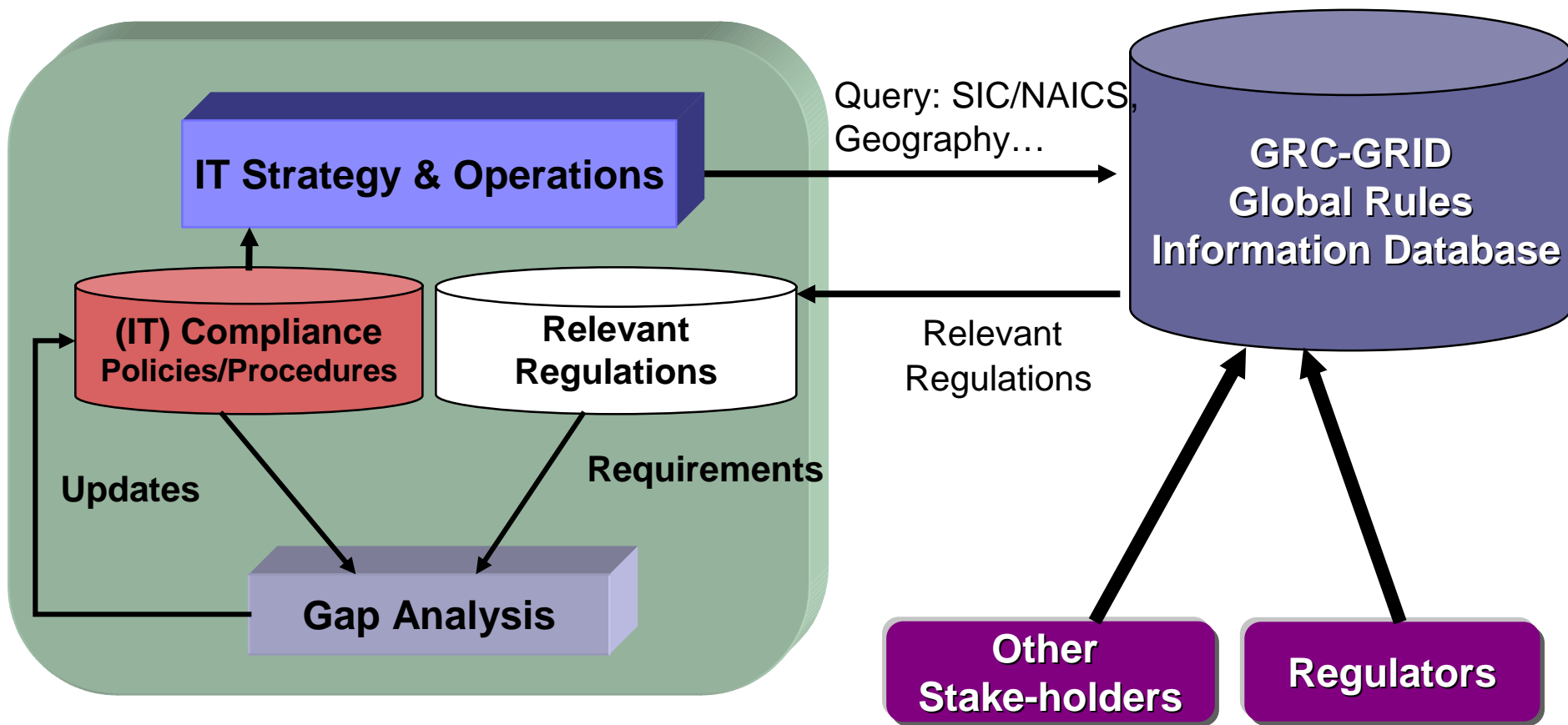
1. Capture and Catalog the Requirements
2. Capture the interdependencies between regulatory requirements and indicated IT controls (COBIT, ITIL...)

The C-GRID will provide a dynamic mapping that allows IT management to ensure that regulatory requirements are met, and that the impact of changes to controls are predictable

3. Provide standards-based tools to help end-users continually monitor regulatory changes and respond effectively (Tools built by GRC-GRID sponsors can leverage the open GRC-GRID platform to provide these services)
4. Automate the capture of GRC information (working with the regulatory agencies)

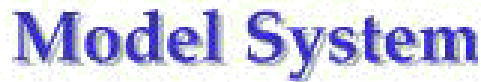
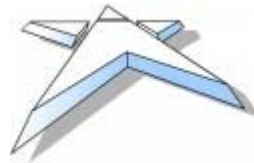
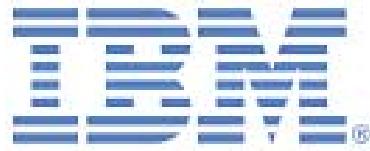


The Next Frontier



Ultimately, The GRC-GRID will automatically receive updates from the regulators and framework/policy updates from the GRC-RT community.

The Design Was Collaborative...



Business Semantics Ltd



Implementation and Operations are Collaborative, Too.



US NATIONAL
ARCHIVES



Already received compliance and privacy data on over 100 countries from individuals, top tier banks and brokerage firms...currently in discussions with additional:

- *Global audit firms*
- *US and European Universities*
- *Global professional service firms*
- *Additional not-for-profit organizations and dozens of the largest user organizations.*



The Global Rules Information Database

developed for the
**Governance, Risk Management
& Compliance Roundtable**

**Adrian Bowles, Ph.D.
Said Tabet, Ph.D.**

Object Management Group
<http://www.omg.org>

