

IT Focused Governance, Risk and Compliance

Professor Wendy Currie
CIO Symposium
8 June 2011
Helsinki, Finland

Definitions of GRC

- ▶ **Enterprise Governance Risk & Compliance (EGRC) —**
The primary purpose of the EGRC platform is to **automate** much of the work associated with the documentation and reporting of the **risk management and compliance** activities that are most closely associated with corporate governance and business objectives.
- ▶ **IT Governance Risk Compliance (IT GRC) -** The management, measurement, monitoring, automation and reporting of **IT controls**
- ▶ **Governance Risk Compliance Management (GRCM) -**
The automation of the management, measurement, gap remediation, and reporting of controls and risks against objectives, and in accordance with **rules, regulations, standards and policies.**

(Caldwell 2010; Nicolett, & Proctor 2010; Harris et al 2010)

GRC in 2011

- ▶ The once-prevalent view of IT governance as a **stand-alone entity**, distinct and separate from corporate governance, is fading fast (Bace et al 2011).
- ▶ Drivers for GRC emanating from the Economic Crisis:
 - Increased **regulatory requirements** across industries.
 - Increased need to demonstrate **transparency** to shareholders.
 - **Reduced IT budgets** require more cost effective and efficient IT assets/spend.
- ▶ Chartis Research forecasts the worldwide financial services OpRisk and GRC technology market will grow to **\$2 billion by 2013** at a compound annual growth rate of 6.5%.

GRC Platform Vendor Market

- ▶ The GRC platform vendor market is seeing dramatic growth from a \$635 million global market in 2009 to a nearly \$749 million market in 2010

The Forrester logo consists of a dark green oval with the word "FORRESTER" in white, uppercase, serif font. A registered trademark symbol (®) is located to the right of the word. The logo is positioned in the lower right area of the slide.

FORRESTER®

GRC Research

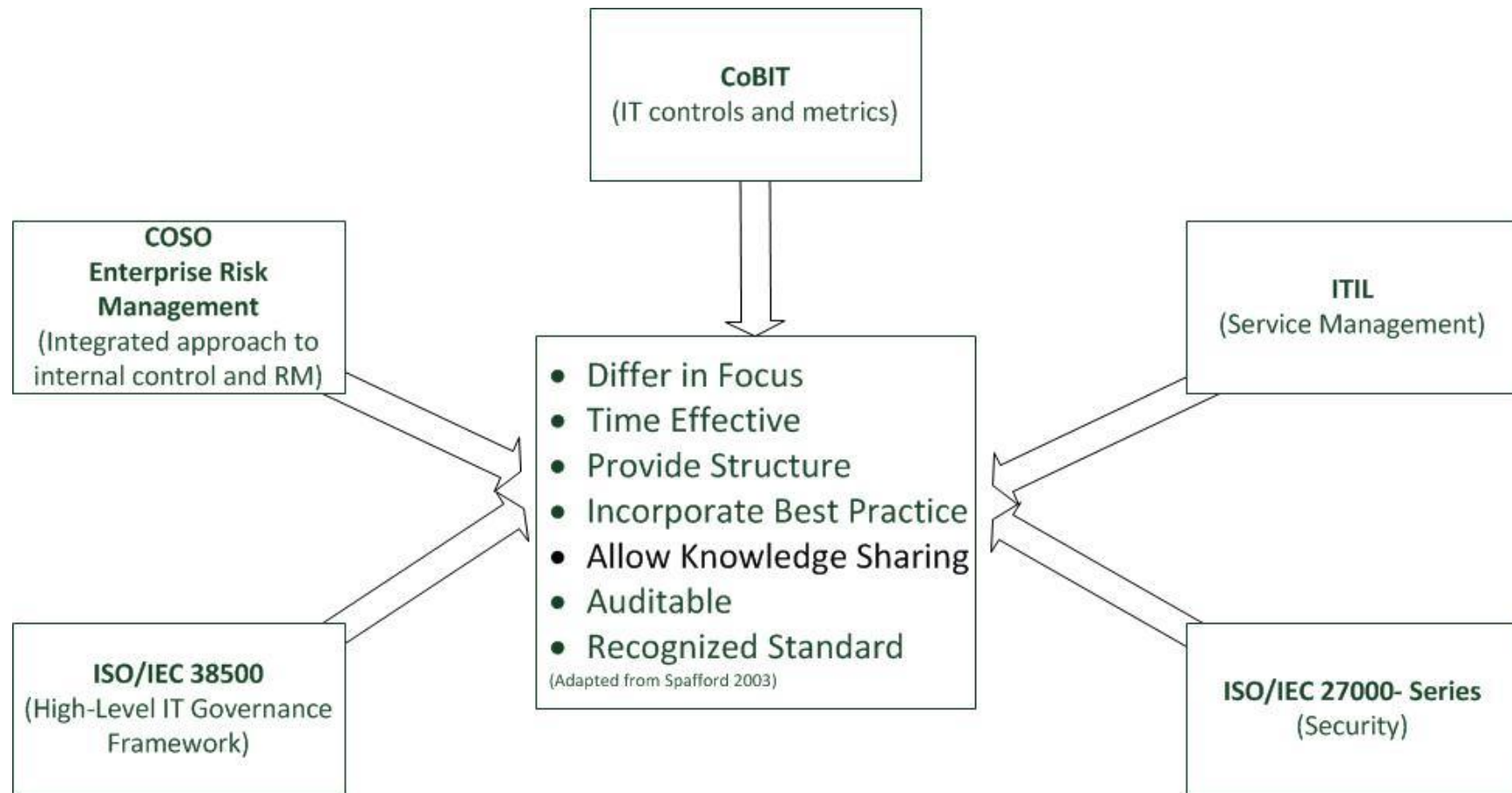
- ▶ Little empirical research into GRC.
- ▶ 3-Year research project focusing on:
 - Dissemination of best practice, how and why?
 - How organizations make sense of new regulatory requirements and understand their exposure to new mandates from an IT perspective.
 - The role of outsourcing in GRC.
- ▶ Presentation highlighting some preliminary findings at ECIS 2011 – (Currie, Finnegan, Gozman- Accounting information systems as institutional carriers: a case study of regulatory compliance in UK asset management houses)



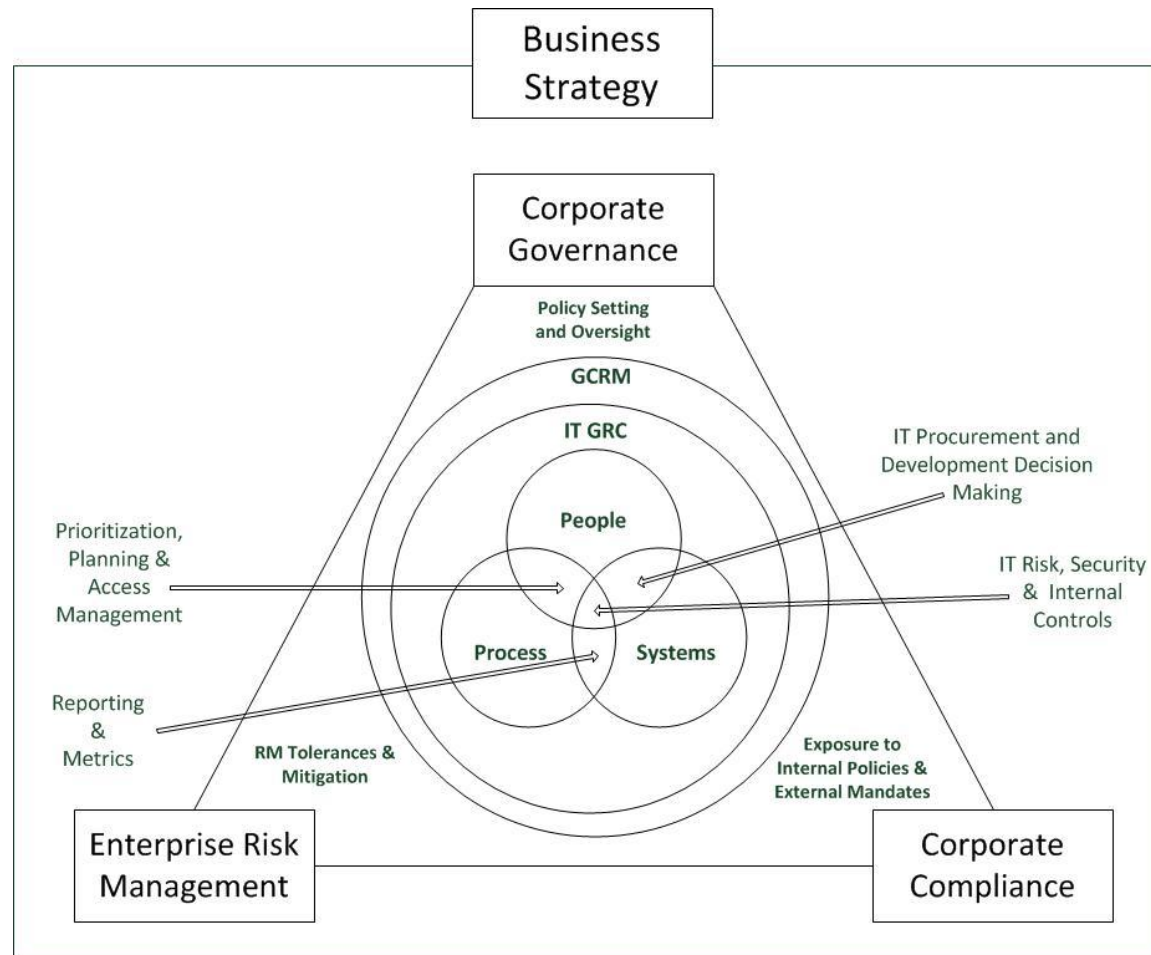
GRC Questions

- ▶ What upcoming regulatory changes impact my organization and what is the role of IT in the remediation process?
- ▶ How mature and aligned is the organization's GRC capability and what is the role of IT and industry standards?
- ▶ What data is required to run necessary controls and what systems need to share this data?
- ▶ What existing IT assets can provide GRC and what are the gaps in required functionality?

A Medley of Frameworks for IT GRC



Aligning GRC Activities



The Evolution of IT Outsourcing in Financial Services



Over the years, outsourcing has evolved and spawned a plethora of new delivery models and managed service options for various IT-related functions, from off-shoring to “XSPs” (Application Service Providers, Managed Service Providers, and so on) followed by the wave of “XaaS” options (Software as a Service, Infrastructure as a Service, etc.).

From Traditional to Best Sourcing

Traditional Outsourcing

- ▶ Lower cost – organizations can reduce up-front investment and ongoing costs by tapping into a service provider's existing economy of scale in hardware, infrastructure, and IT support resources.
- ▶ Predictable costs and service levels – outsourcing makes it easier to predict and limit exposure when IT is called upon to support new business initiatives.
- ▶ Scalability – outsourcing increases flexibility by enabling an organization to add or remove capacity incrementally.
- ▶ Focus – for many organizations, outsourcing non-strategic applications allows them to focus on their core competency.

Best Sourcing

- ▶ Time to market – utilizing a provider's expertise and existing application delivery infrastructure enables firms to be more agile and enter markets faster.
- ▶ Higher core application utilization and value – a core solution provider with expertise in the application and related areas can apply best practices and tailor them to a firm's unique business needs in ways that increase application utilization and improve end-user satisfaction.
- ▶ Increased business responsiveness – access to dedicated application experts helps firms stay more current with technology-enabled industry best practices and changing regulatory requirements.

Managed Services

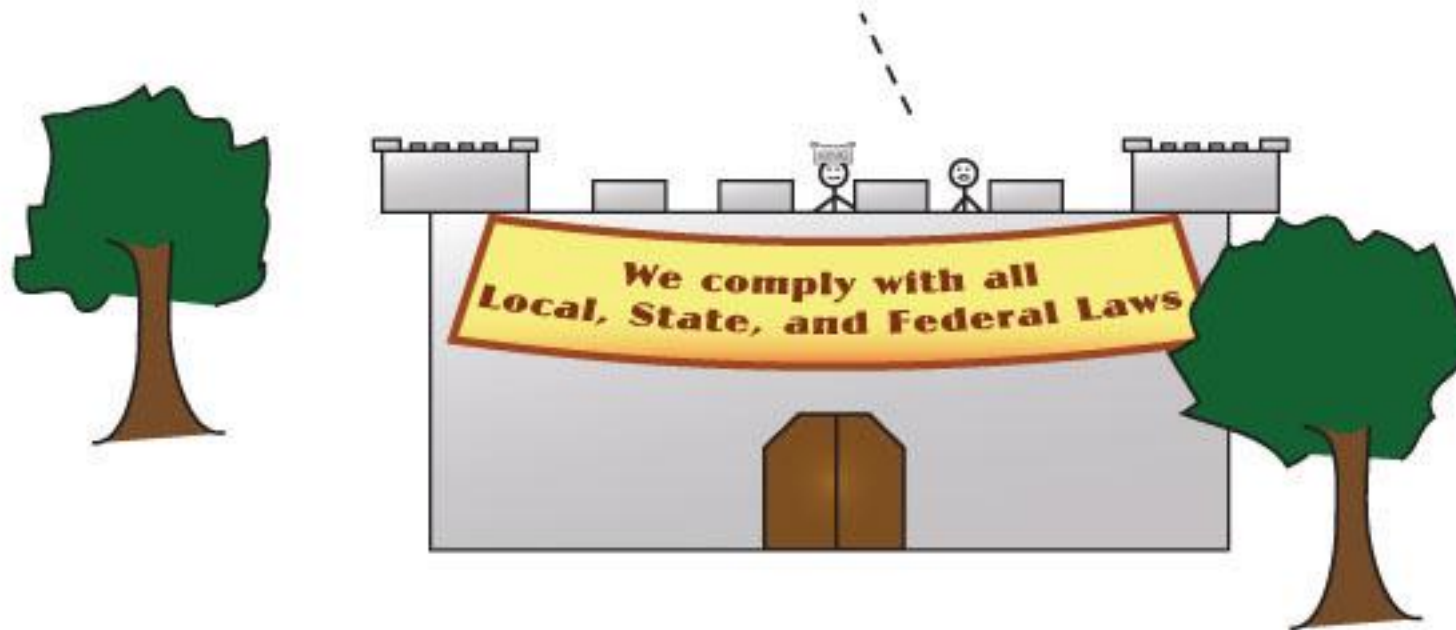
- ▶ Expertise in implementing, tailoring and managing the front-office platform
- ▶ Experience working with buy-side firms similar in size, business model and areas of focus
- ▶ Ability to provide deep application expertise on a 24x7 basis – to support global operations if applicable, or at a minimum to provide off-hours support and vacation/holiday coverage
- ▶ Predictability of cost and reasonable terms for incrementally adding/removing capacity or services, as well as scalability to support growth initiatives
- ▶ Ability to provide support throughout the investment lifecycle, from decision support and portfolio management through execution, post-trade settlement and performance measurement, attribution and risk analysis
- ▶ Longevity and stability in the market
- ▶ Reputation for technical support and customer service

Preliminary Conclusions

- ▶ Set up a committee of stakeholders to understand the impact of new regulations, such as Dodd-Frank, at the industry, firm and the IT levels.
- ▶ Business and IT to build cross-functional relationships with legal, audit and finance depts.
- ▶ Ensure that existing IT governance standards, practices and programs are aligned with GRC requirements as well as corporate governance and business objectives.
- ▶ No single IT vendor solution can provide complete GRC.
- ▶ Prepare to meet increased auditing requirements
- ▶ Data is key:
 - Pay particular attention to data required for risk management calculations and for structuring and imposing rules for financial transactions.
- ▶ Organizations with similar regulatory exposures and systems may benefit from sharing experiences.
- ▶ Address skills shortage of IT compliance staff – more focused training
- ▶ ASP, SaaS finally making an impact in GRC as ‘managed services outsourcing’

Legal, Regulations, Investigations, and Compliance

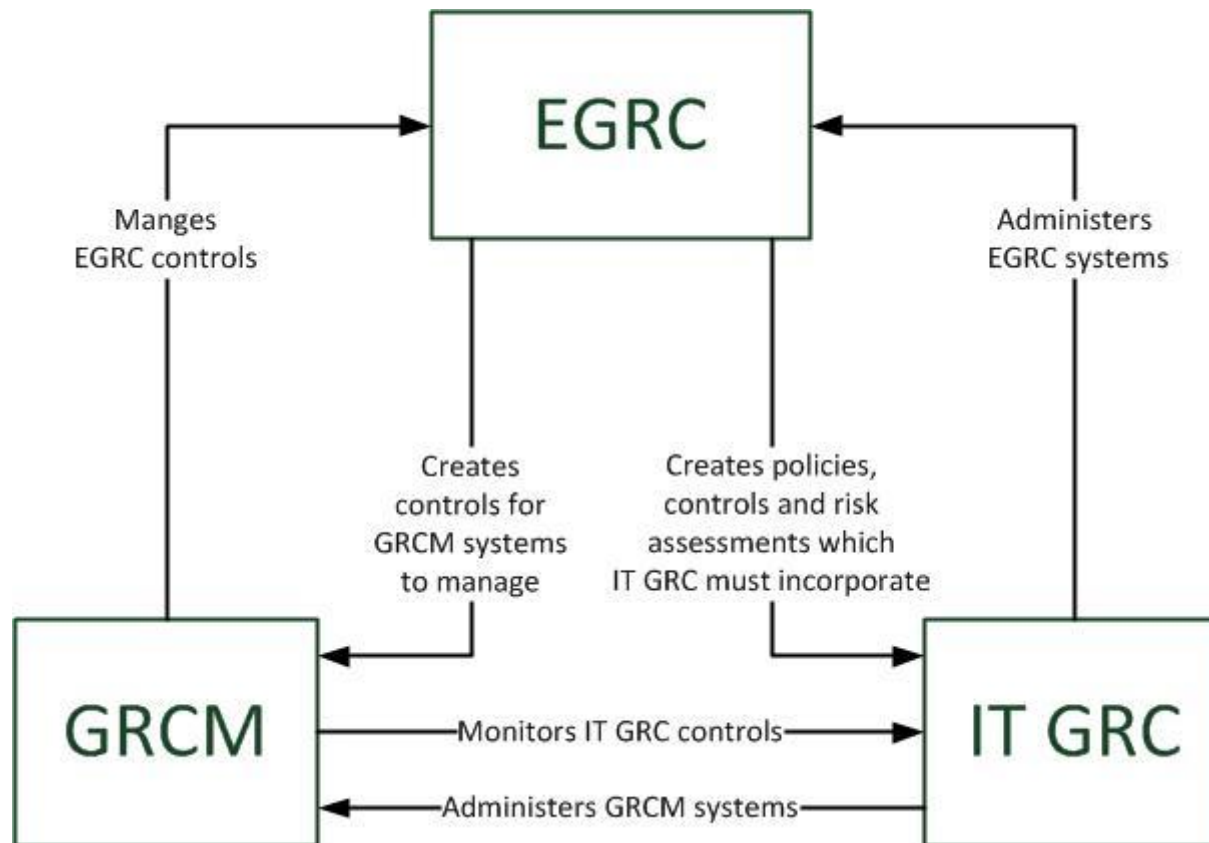
You really think the auditor will believe this, Sir?

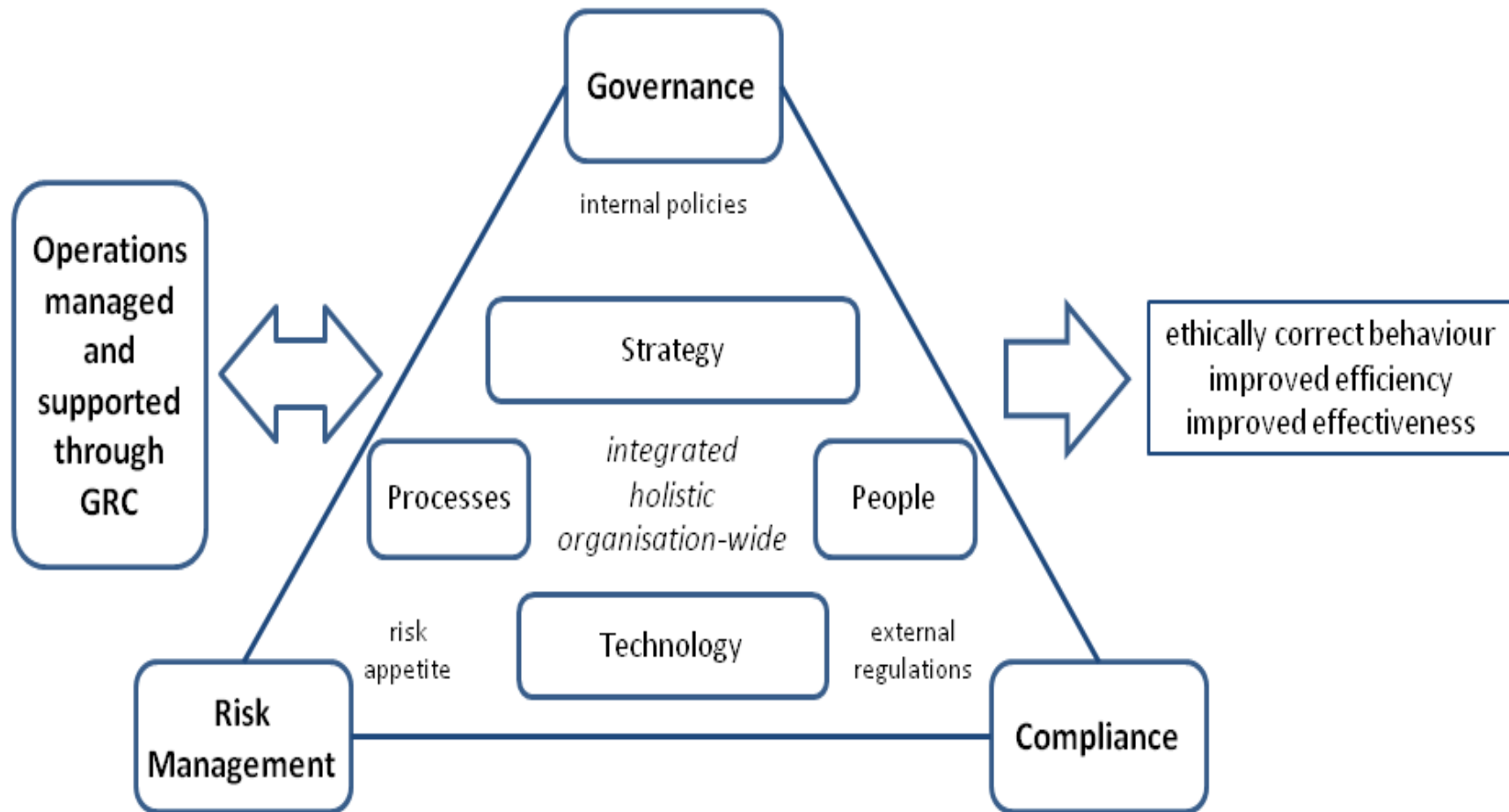


References

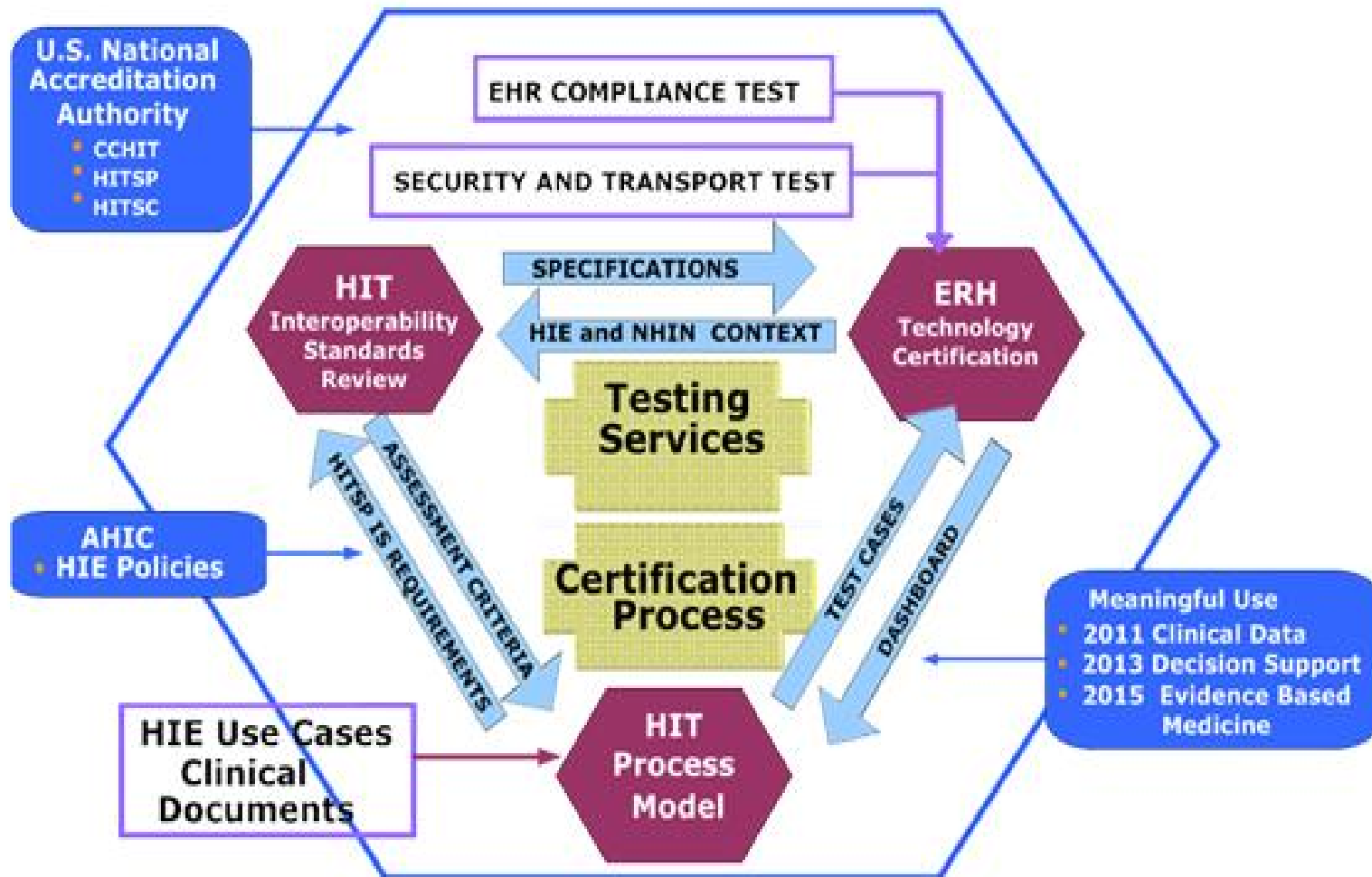
- ▶ Bace, J., Wheatman, J., Scholtz, T., Short, J., Burton, B., and Caldwell, F. 2011. "Predicts 2011: In the 'New Normal,' Governance, Risk Management and Compliance Are Inseparable from Business Realities," Gartner Research (17th November).
- ▶ Caldwell, F. 2010. "Magic Quadrant for Enterprise Governance, Risk and Compliance Platforms," Gartner Research (13th October).
- ▶ Chartis Research. 2010. "Operational Risk & Grc Software Solutions 2010." Retrieved 24th February, 2011, from <http://chartis-research.com/research/reports/operational-risk-grc-software-solutions-2010>
- ▶ Harris, K., Hunter, R., Gomolski, B., Gerrard, M., and Proctor, P.E. 2010. "The New Realities of It," Gartner Research (17th August).
- ▶ Nicolett, M., and Proctor, P.E. 2010. "Critical Capabilities for IT Governance, Risk and Compliance Management," Gartner Research (30th April).
- ▶ Proctor, P.E., and Caldwell, F. 2011. "A Comparison Model for the GRC Marketplace, 2011 to 2013," Gartner Rserach (23rd March).
- ▶ Spafford, G. 2003. "The Benefits of Standard It Governance Frameworks." Retrieved 23rd May, 2011, from <http://www.itsmwatch.com/itil/article.php/2195051>

GRC Activities: Mutually Supportive





IT Compliance and Healthcare



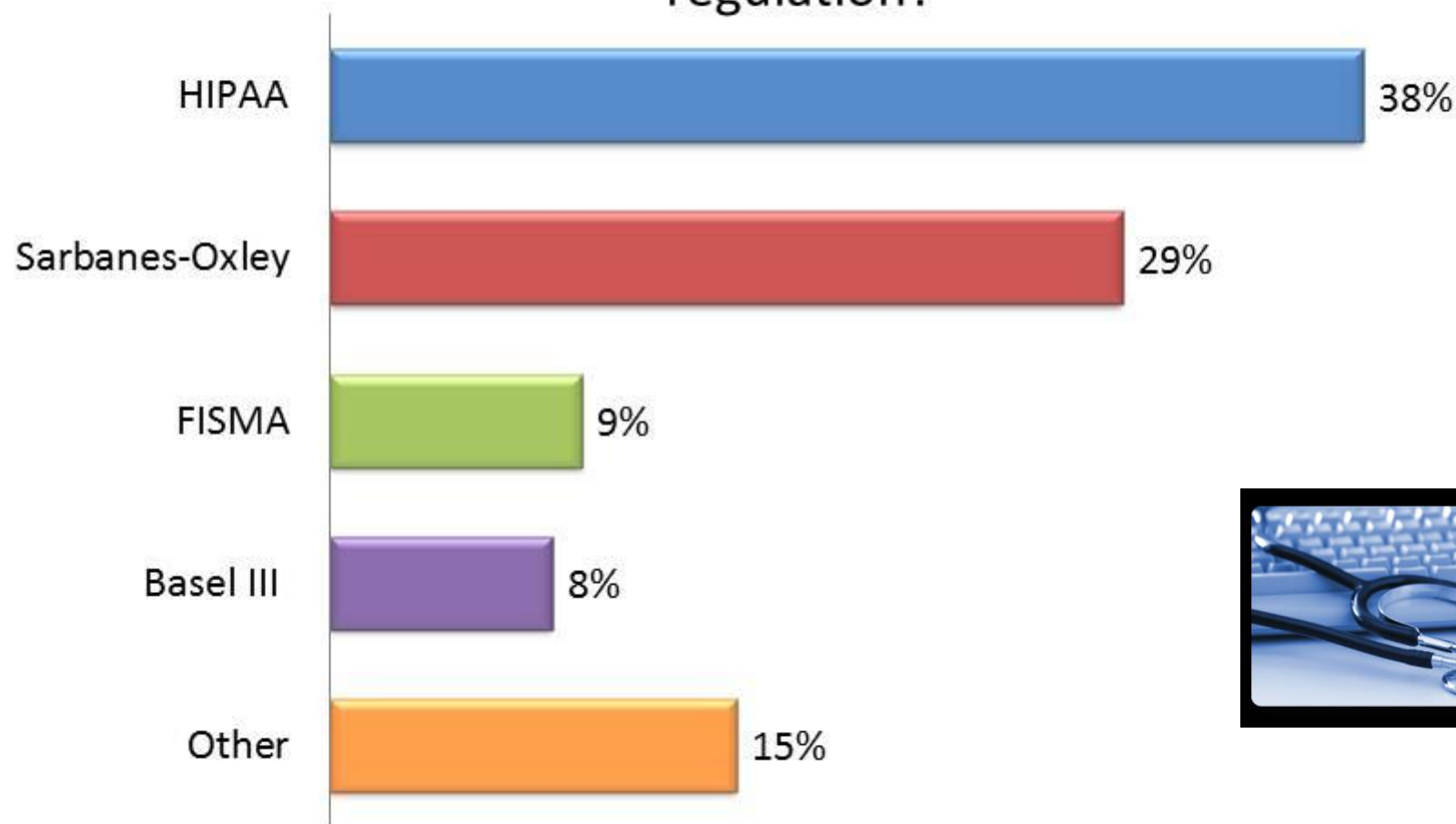
© Mike Baldwin / Cornered



“Somehow your medical records got faxed to a complete stranger. He has no idea what’s wrong with you either.”



From an IT standpoint, what is the most challenging compliance regulation?



Source: Ipswitch Inc.'s Network Management Division