Designing and Operationalizing Corporate GRC Infrastructure:

Challenges, Strategies and Tools

Austine J. Ohwobete

(PhD, CISSP, CISA, CEH, CHFI)

Austine.ohwobete@rhi.com

October 2012

Presentation **Menu:**

- GRC: A Brief Introduction
  - Governance
  - Risk Management
  - Compliance
- Enterprise GRC: What is at stake
  - A research insight:
    - The drivers
    - The current state of implementations
    - Typical Scope of implementations
- Operationalizing the Enterprise GRC:
  - The challenges
  - The strategies
  - The tools
- Last Word on Enterprise GRC
- Questions (and some answers, perhaps)?

Governance: What it means

"A governance system is all the means and mechanisms that will enable multiple stakeholders at various levels of an entity for specific purposes to have an organized say in setting direction and monitoring compliance and performance so as to create for them acceptable value, while taking acceptable risk levels and using limited resources responsibly."

- Key implications of the definition:
  1. The necessity of a framework,
  2. The essentiality of a set of guiding principles,
  3. The inevitability of a structure,
  4. The obligation to institute processes; and
  5. The establishment of core practices

Enterprise GRC: The Governance Component

Governance facilitates setting business strategy & objectives, determining risk appetite, establishing culture & values, developing internal policies and monitoring performance.

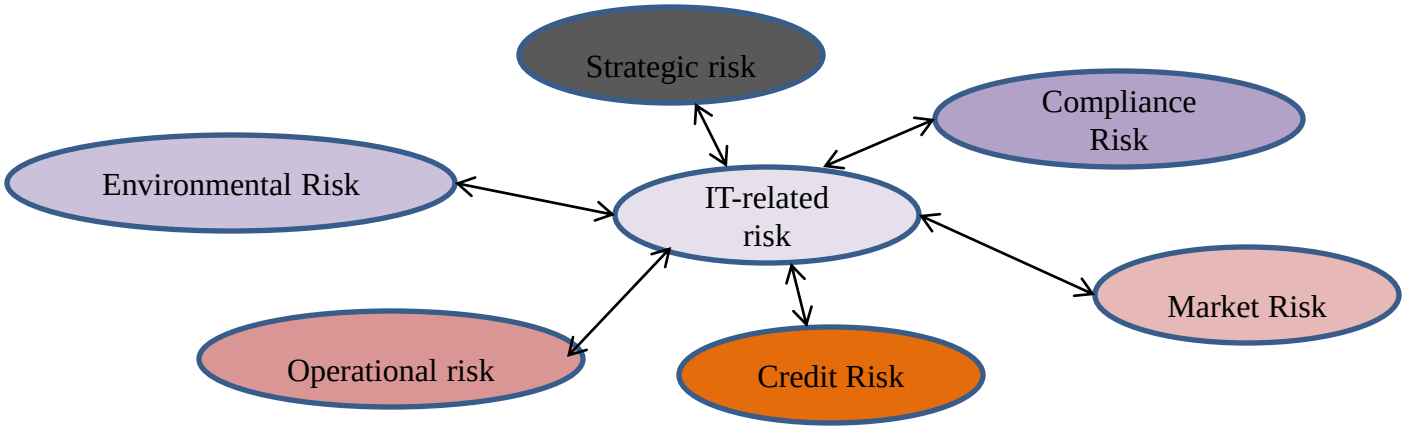
Governance is concerned with accountability and responsibility in terms of the standards that are used to direct and control an operational unit of the enterprise.

- What it means:
  - Denotes steering, and includes the exercise of legal and regulatory authority and the use of institutional resources to manage organizations.
- What it does:
  - Addresses the processes, systems, and controls by which organizations, both public and private, operate.
- What it involves:
  - Who is governing
    What is being governed
    The resources/assets deployed in the process

Enterprise GRC: The Risk Component

- Risk refers to the possibility of a loss or an injury created by an activity or by a person
  - Risk management – RM – seeks to identify, assess, and measure risk and then develop countermeasures to handle it.
    - This typically does not mean eliminating risk but rather seeking to mitigate and minimize its impact.
    - Risk should not be viewed as inherently bad.
    - An organization that is totally risk averse is not likely to be very attractive to investors and may be doomed ultimately to fail.

Categories of enterprise risks:



Enterprise GRC: The Compliance Component

- Defined by the Compliance and Ethics Leadership Council as:
  - A company or an individual's observance of relevant laws, regulations, and corporate policies
- According to the DOJ,
  - Compliance programs are established by corporate management to prevent and to detect misconduct and to ensure that corporate activities are conducted in accordance with all applicable criminal and civil laws, regulations, and rules.
- Key compliance ingredients:
  - An effective compliance program
  - Sufficient and aligned compliance performance incentives
  - Emphasis on the consequences of noncompliance
  - Non-generic, customized training that is focused on influencing employee behavior

Ensuring Compliance: the seven steps approach

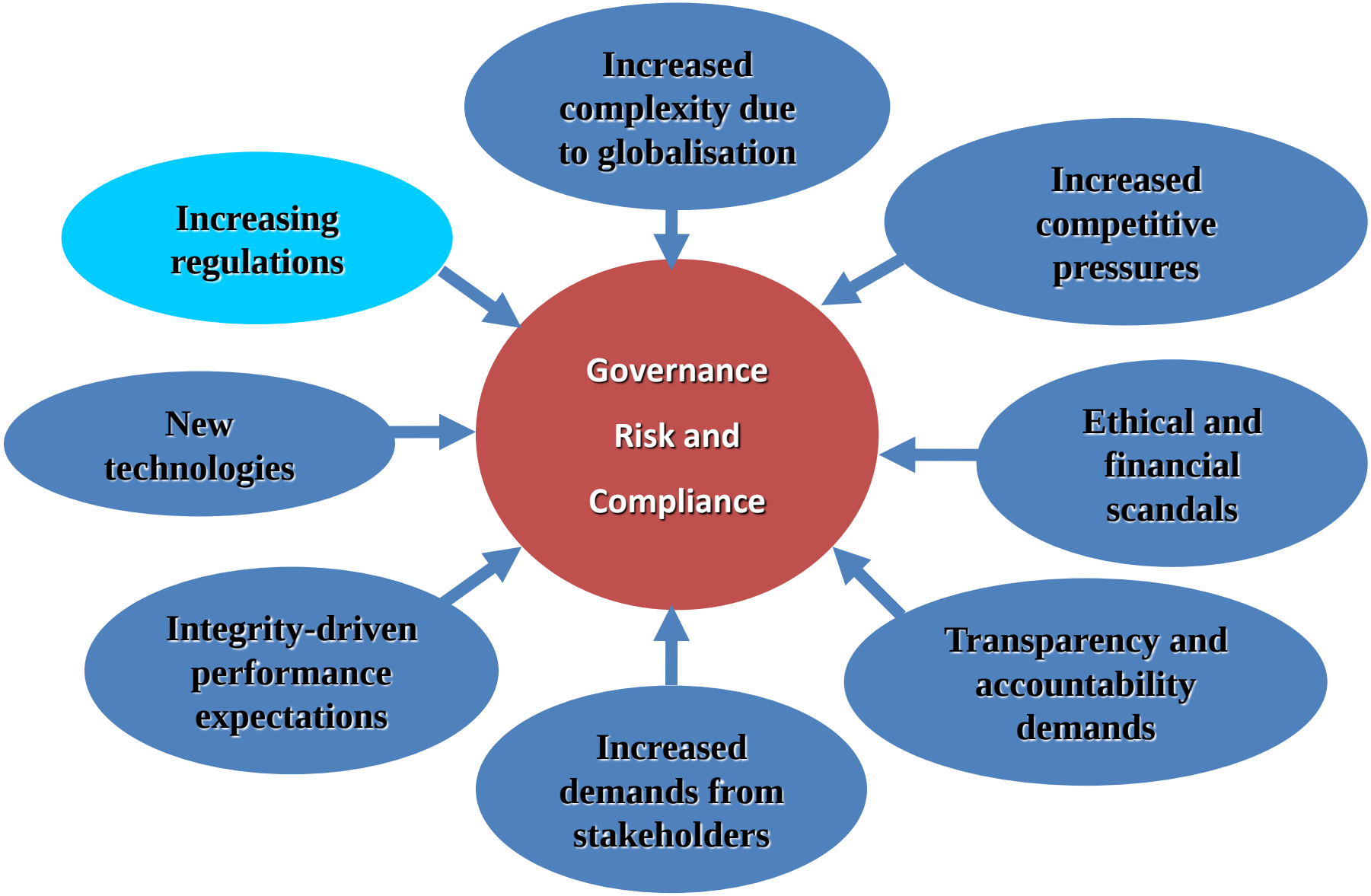
As mandated by the FSGO, organizations can build and maintain an effective compliance and ethics program by following the steps outlined below:

- Establishing compliance standards and procedures
- Organizational leadership and a culture of compliance
- Reasonable efforts to exclude prohibited persons
- Training and communication of standards and procedures
- Monitoring, auditing, and evaluating program effectiveness
- Performance incentives and disciplinary actions
- Response to criminal conduct and remedial action

Enterprise GRC: What is at stake

- Huge Investments in GRC Initiatives.
- Primary Drivers:
  - Compliance Obligations
  - Regulatory Mandates
- The Catch:
  - Validating/Justifying the Investments
  - *Cutting-edge GRC Tools often do not Guarantee Success*.
- What is Missing:
  - An Effective Strategy based on 360 Degrees Collaborate

Business drivers for an integrated approach to Governance, Risk and Compliance



Research Insight: Drivers of IT GRC Implementations

Source: TechTarget © 2012

Research Insight: Scope of IT GRC Implementation

E-Discovery

Data Quality

Information Lifecycle

Records Management

Data Protection

All of the Above

0% 10% 20% 30% 40% 50%

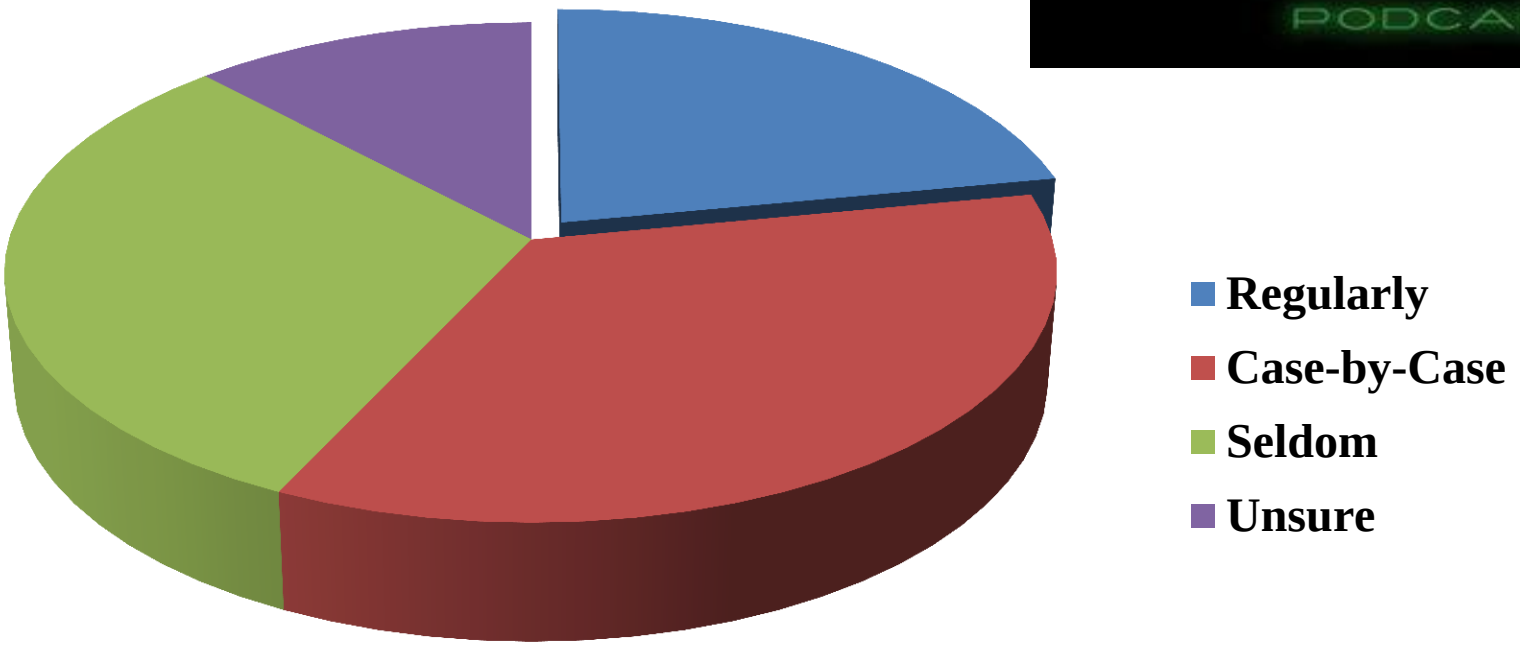
Source: TechTarget © 2012

Research Insight: Status of IT GRC Implementations

- Already Implemented
- Currently Implementing
- Plan to Implement next Year
- No current plan to implement

Source: TechTarget © 2012

Research Insight: Freq of Meeting to Discuss GRC Issues



Source: TechTarget © 2012

Enterprise GRC Challenges: The View from the top

• CFO / VP Finance

- Timely notification of control issues, material weaknesses and violations
- Accurate and comprehensive information on financial exposure, compliance and audit.
- **Reducing the total cost of GRC*****
- Timely notification of control issues, material weaknesses and violations
- Accurate and comprehensive information on financial exposure, compliance and audit.

• Chief Compliance Officer (CCO)

- Reducing regulatory actions by reducing compliance violations
- Planning and oversight of compliance management resources
- Identifying and implementing optimal detective & preventative controls
- **Increasing efficiency & consistency of compliance processes*****
- Reducing regulatory actions by reducing compliance violations
- Planning and oversight of compliance management resources
- Identifying and implementing optimal detective & preventative controls

Enterprise GRC Challenges: The View from the top

Chief Risk Officer (CRO)

- Evaluating business requirements and technical risk capabilities
- Reducing organizational cost of risk exposure and cost of mitigation or acceptance
- **Balancing the range of enterprise risks*****
- Evaluating business requirements and technical risk capabilities
- Reducing organizational cost of risk exposure and cost of mitigation or acceptance

CIO

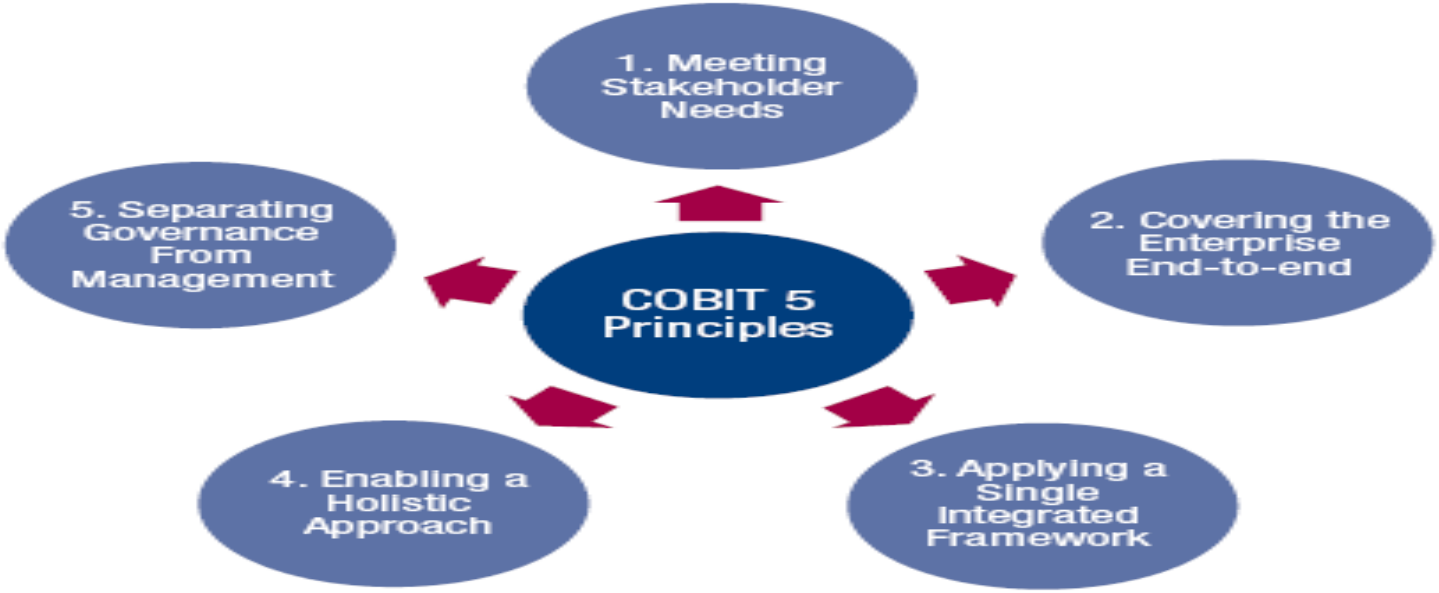
- Automating GRC information risk management
- Eliminating multiple internal GRC solutions
- Implementing IT platform for GRC standardisation, simplification & security
- **Ensuring Auditable secure information*****
- Automating GRC information risk management
- Eliminating multiple internal GRC solutions
- Implementing IT platform for GRC standardisation, simplification & security

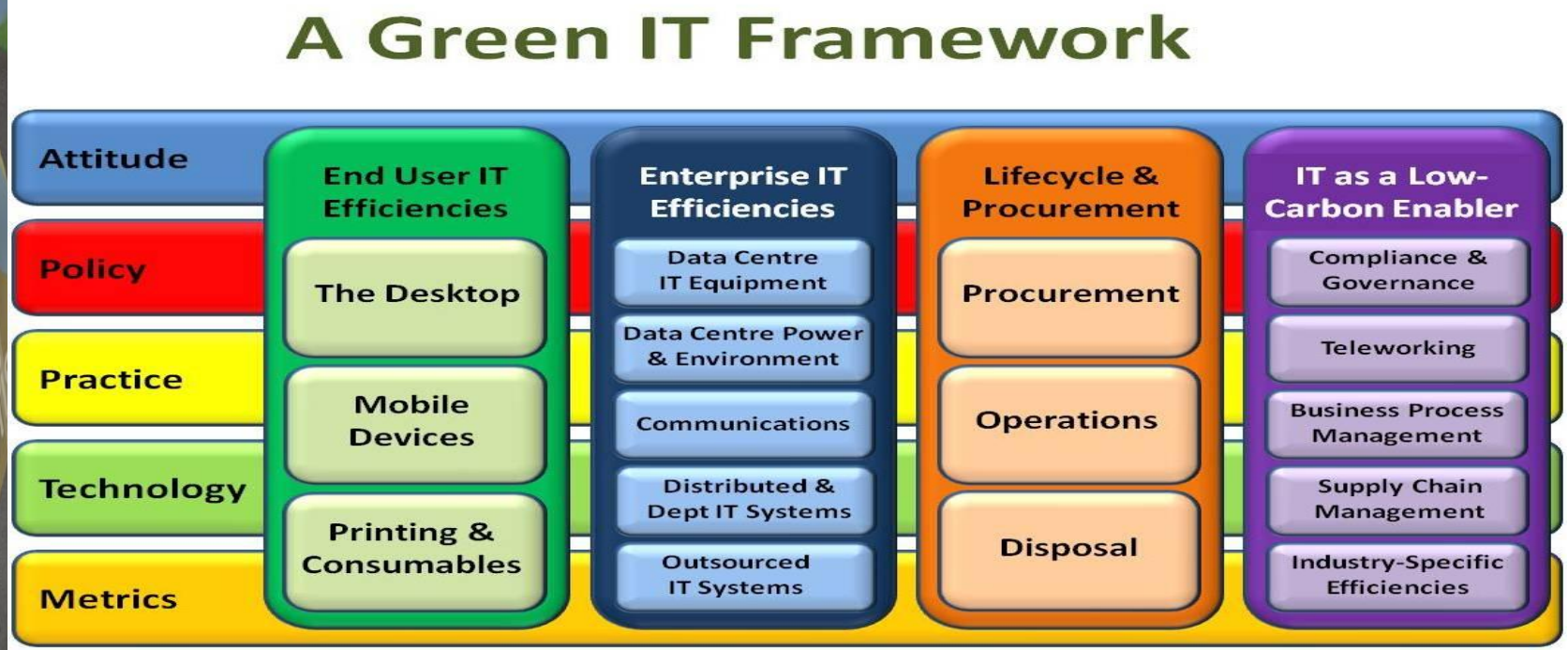
Implementing Enterprise GRC: Before the Rain

As with most enterprise-wide initiatives, implementing an enterprise GRC program requires a coordination of different and sometimes opposing objectives, expectations, and resources. Therefore:

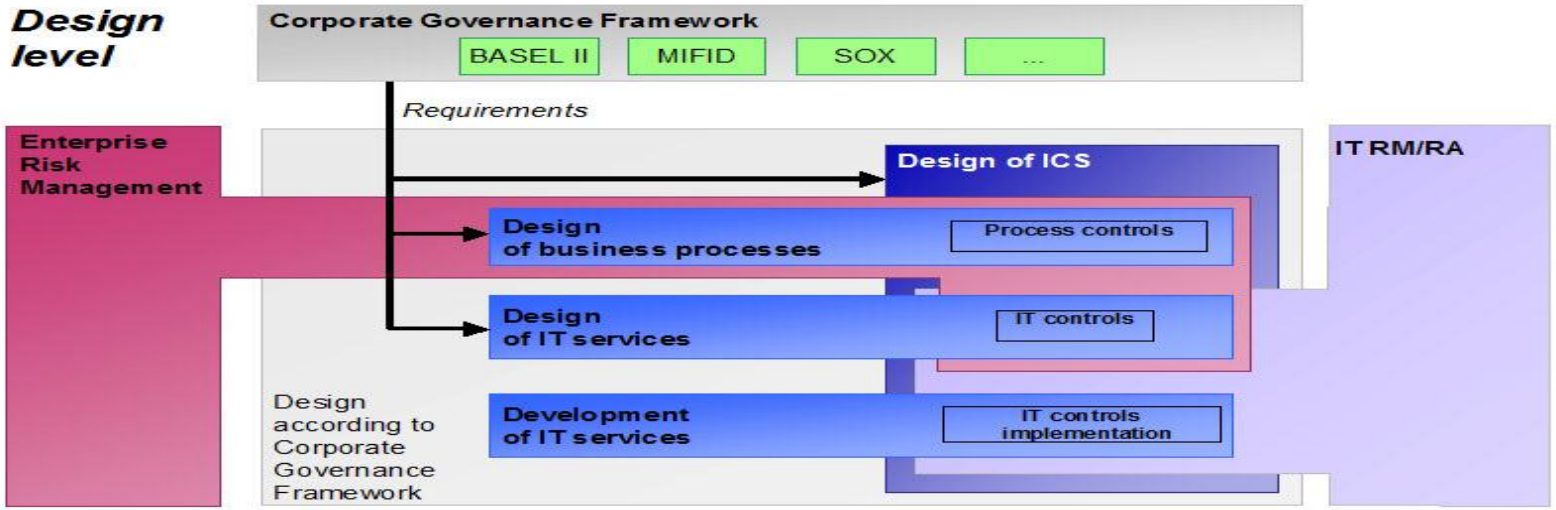
- Become a GRC salesperson:
  - Knowing that the success of any broad implementation requires executive sponsorship, as well as participation from business process owners, it is important to anticipate opposition and obstacles
- Remember the basics of project management:
  - It is imperative to set and track objectives, milestones and deliverables: it is not enough to have initial buy-in from executive sponsors and business process owners
- Embed GRC into the culture:
  - Selling key stakeholders on the business value of GRC and having an airtight project plan will get the process rolling, but true success in GRC can only occur if it ingrained within the culture of the organization

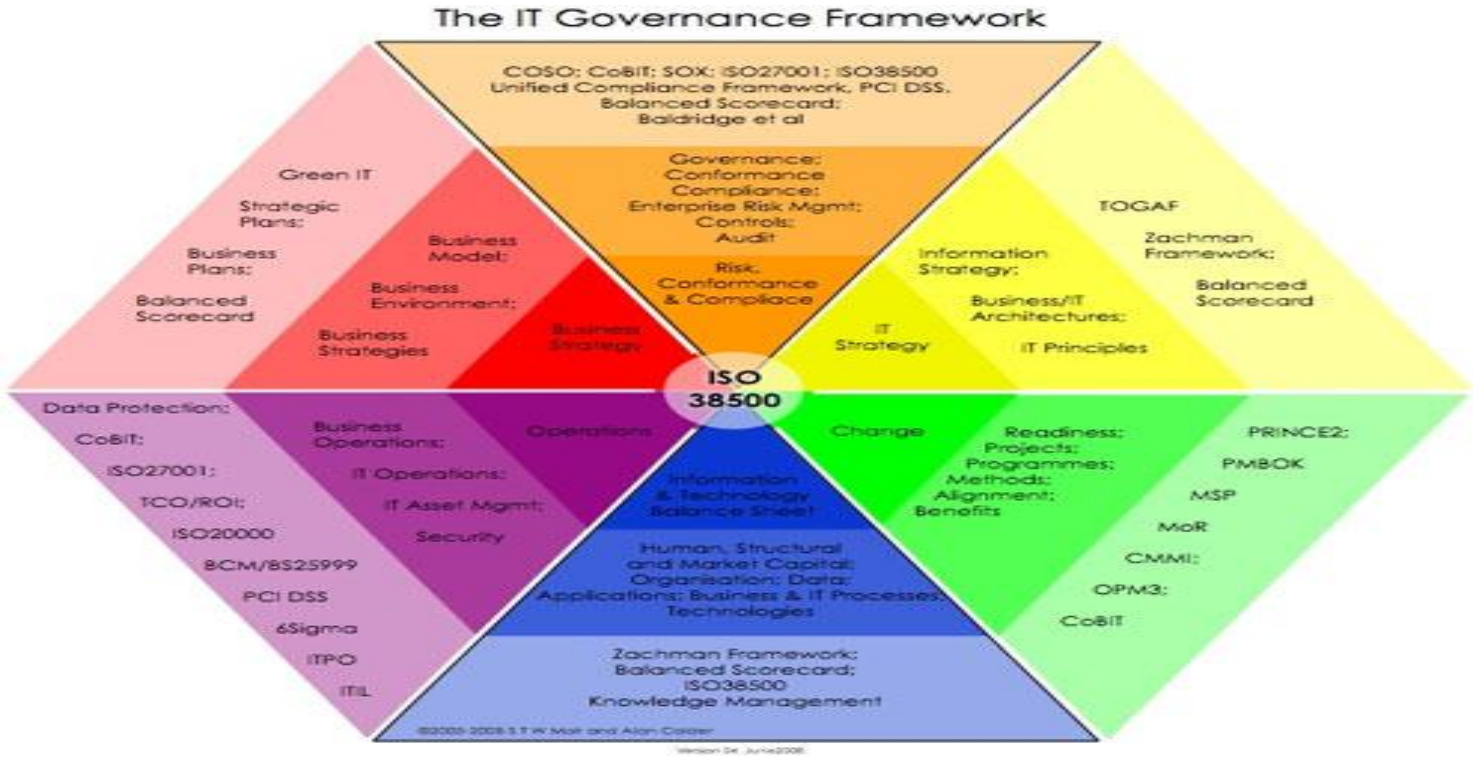
Implementing Enterprise GRC: Frameworks



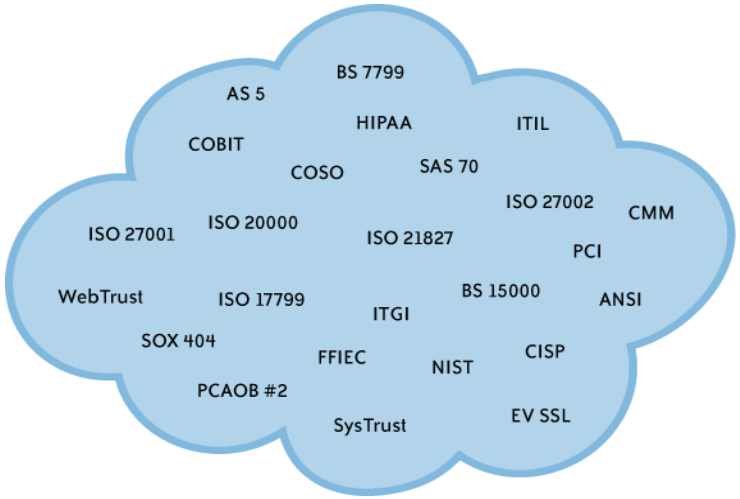


Implementing Enterprise GRC: Frameworks





Implementing Enterprise GRC: Frameworks



Frameworks - Models - Maps

conceptualising and structuring insights, information and knowledge

Generic Frameworks

Such as

Exisiting/Accepted frameworks; compelling experience, Think | Do | Use, compliance triangle

Good for

- Structuring thinking, ordering thoughts
- Attacking/dealing with the volume of initial information

Specific Frameworks

Such as

Frameworks developed from previous research and service design activity

Good for

- Scoping based on intent from known customer, business, technology angles

Directive Frameworks

Such as

Frameworks developed from research undertaken for the current service design activity

Good for

- Capturing directional thinking
- Aligning to identified contextual insights, design criteria
- Communicating insights and progress

Directive Maps

(aka pathways, journeys)

Such as

Synthesised experience representations such as customer experience maps, service blueprints

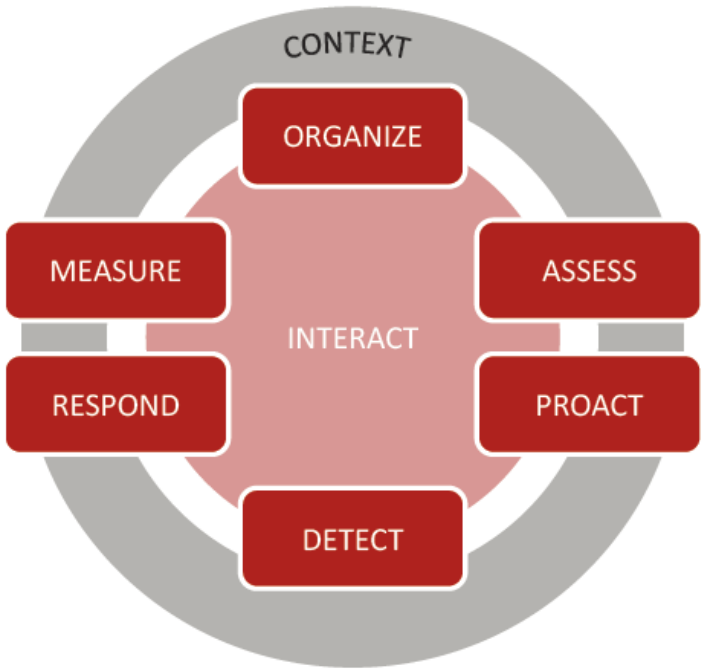
Good for

- Describing customer experience aligned to the intent of the design goal
- Prototyping and communicating

desonance

The OCEG Red Book GRC Capability Model version 2.1: A GRC Implementation Model

8 INTEGRATED COMPONENTS



8 UNIVERSAL OUTCOMES

- Achieve Business Objectives
- Enhance Organizational Culture
- Increase Stakeholder Confidence
- Prepare & Protect the Organization
- Prevent, Detect & Reduce Adversity
- Motivate & Inspire Desired Conduct
- Improve Responsiveness & Efficiency
- Optimize Economic & Social Value

Enterprise GRC: Implementation Strategies

- Take a Holistic approach
  - An expensive and painful approach is to treat it in a piecemeal and disjointed fashion, as a series of unrelated tasks, as an unfair and added cost with few tangible benefits.
    - Treat it as a strategic imperative and key to the growth of the organization
- Map processes to controls to audited regulations
  - By mapping the process, risk, control, audit test, and regulations, an organization can avoid redundant compliance costs by using one control and audit test for multiple regulations
    - This also helps to make the business case for standardizing and automating the control and testing process
- Rationalize and prioritize risks
  - This can be as simple as creating a scoring system for three or more variables of risk such as economic impact (severity), likeliness of occurrence (frequency), and ability to detect (discovery)
- Increase controls standardization and automation
  - Automated controls lower costs and lower risks, and further, process improvements go hand in hand with automation.
- Create an internal controls grading system for IT systems

Implementation Strategy

A 360-Degree Approach Via Principled Performance

Enterprise GRC: Implementation Strategies

- Governance:
  - Ensure that sound governance structures are in place “below the board” so that the right information about the right issues is available at the right time
- Risk:
  - Integrate risk management with strategic planning and maintain a 360-degree view of organizational risks and effectively allocate resources to address them
- Ethics and Compliance:
  - Establish practices and a culture to prevent misconduct, inspire desired conduct, detect problems and improve outcomes

Enterprise GRC: Implementation Strategies

- Finance:
  - Reduce costs and optimize how you allocate capital to governance, risk and compliance processes so that GRC is better aligned with the business
- Technology:
  - Address compliance issues and the alignment of information technology to generate GRC needs in the rest of the business
- Audit:
  - Go beyond financial processes and assess the design and operation of controls for governance, risk management, compliance and ethics efforts throughout the enterprise

Enterprise GRC: Implementation Strategies

- Legal:
  - Identify and establish sound practices to address your legal risks and improve your ability to detect and correct issues, while improving your ability to defend the organization.
- Core Processes:
  - Embed sound GRC practices in all lines of business and core processes so that business owners and operators are accountable for GRC success

Managing Enterprise GRC Implementation:
Three lines of defense

- Set expectations for business operations and internal controls
  - Since this group encompasses the largest portion of an enterprise's workforce, setting firm principles here has the potential to greatly improve the organization's risk posture.
  - Establish risk, compliance, security and legal authority
    - This line of defense is responsible for defining the policies, processes and procedures for GRC, while also monitoring for new vulnerabilities that may arise
  - Assign assurance duties to internal audit (IA)
    - This third line of defense operates as an independent entity and provides assurance to the board that the first two lines are conducting, managing and overseeing GRC processes effectively

Enterprise GRC Implementation: The Tools

When it comes to software GRC tools, the watchword is, Caveat emptor!

- Most GRC products were originally built to address specific requirements
  - For specific areas of the business
- Software marketed as comprehensive GRC solutions functioned in fact as standalone tools
  - They may not integrate well with the software that manages mainstream business processes

Enterprise GRC Implementation: The Tools

- Agiliance Continuous Compliance Service
- Arc Logics Axentis Enterprise
- ArcSight Logger 5.0
- AruvioGRC
- Autonomy Risk Management
- BPS Resolver Issues & Actions Tracking
- Brinqa GRC Platform 3.0
- BWise 4.1.2
- Cloud Security Alliance Cloud Controls Matrix Security Controls Matrix
- Clearwell Legal Hold
- Clearwell Transparent Concept Search
- Commtouch Inc. GlobalView URL Filtering

Enterprise GRC Implementation: The Tools

- CommVault Simpana 9
- Courion Compliance Manager for File Shares
- ControlCase Data Discovery (CDD) and ControlCase Asset and Vulnerability Manager
- Dow Jones Anti-Corruption Portal
- EGestalt SecureGRC
- EMC Corp. eGRC strategy
- EnCase Cybersecurity 4.3
- EthicsPoint Adaptive GRC Framework
- EthicsPoint epVisualization Manager
- GFI WebMonitor
- HiSoftware Compliance Sheriff 4.0
- HP TRIM Enterprise Records Management

Enterprise GRC Implementation: The Tools

- IBM InfoSphere Guardium 8
- Kcura Method
- Lancope StealthWatch 6.0
- LockPath Keylight Platform
- Lunarline's Continuous Compliance Monitoring and Reporting platform
- McAfee Risk Management solution
- MetricStream Compliance Management Solution
- Mitratech TeamConnect Enterprise 3.3
- NetWrix Corp. Change Reporter Suite
- OpenLogic Exchange
- Oracle GRC Controls 8.6
- Oracle Identity Management 11g

Enterprise GRC Implementation: The Tools

- QualysGuard Web Application Scanning 2.0
- Redspin Healthcare Information Exchange Security Assessment
- RSA Archer eGRC Platform
- RSA Solution for Cloud Security and Compliance
- SAP BusinessObjects portfolio
- SocialLogix SocialSentry 2.0
- SonicWALL Continuous Data Protection
- SPDX 1.0
- SunGard iWorks
- Symantec Control Compliance Suite 10.5
- Symantec Web Gateway 5.0
- Unified Compliance Framework
- Virtela's Cloud-based Mobile Device Management

- **Example questions:**

Why are we doing this?
What problem are we solving?
Is this actually useful?
Are we adding value?
Will this change behavior?
Is there an easier way?
What's the opportunity cost?
Is it really worth it?

- **Thanks for your time**