Integrated Governance, Risk and Compliance

Brett Curran

Director GRC Practices - Axentis

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Agenda

- What is Governance, Risk and Compliance?
- Key Challenges
- Technology to Support GRC Management
- Starting Points – Think Big, Implement Small
- Business Case
- Planning and Execution
- Key Drivers of Successful Implementations
- Q & A

Key Definitions

Governance management:

- Organized oversight, requiring comprehensive understanding of mandates, clarity regarding associated roles & responsibilities and meaningful/timely performance information - all necessary to hold the organization accountable

Risk management:

- Identification, assessment and ongoing monitoring of risks (real or hypothesized) and controls – not just to limit downside, but also to maximize opportunity

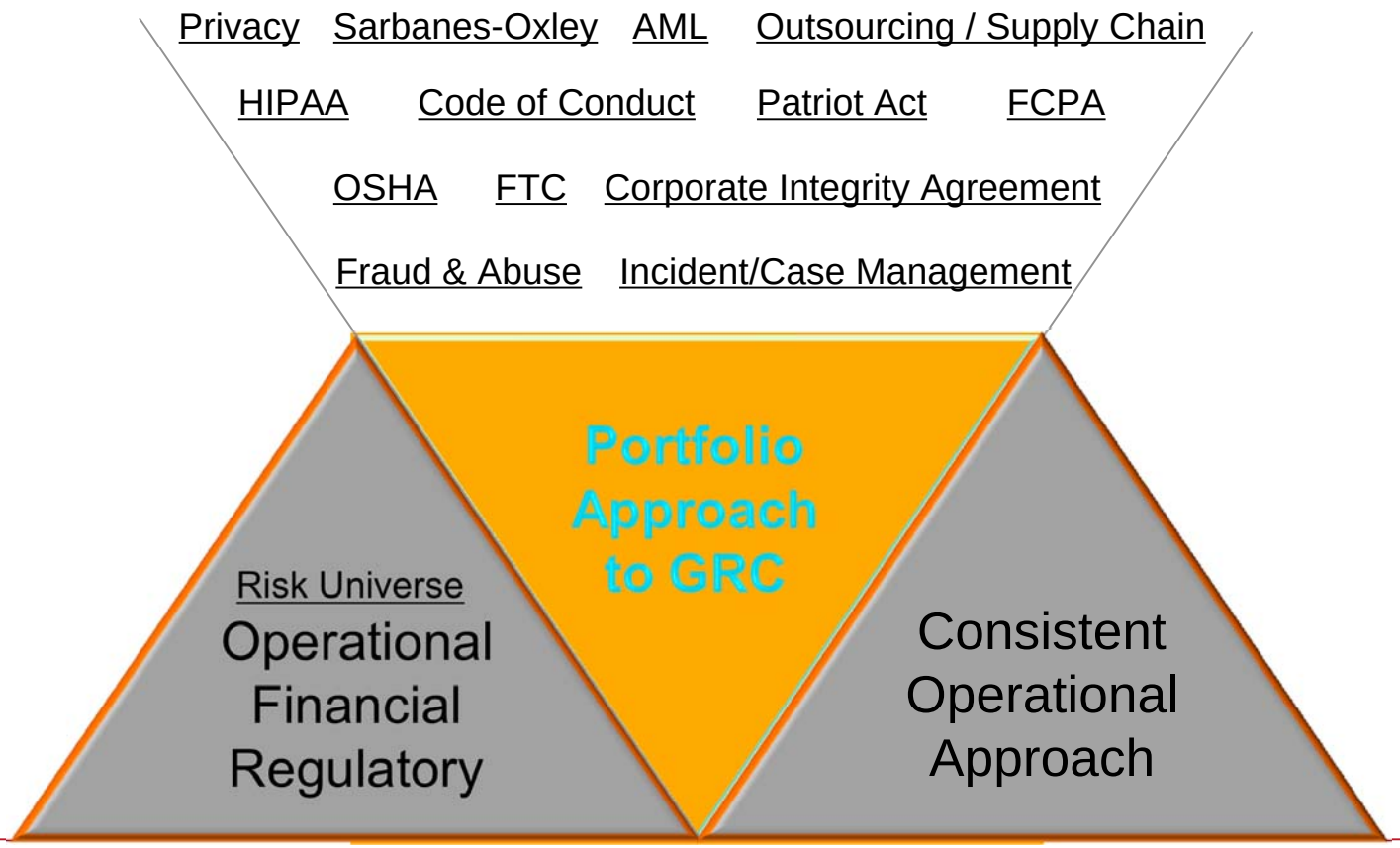
Compliance management:

- Execution of business processes designed to control/manage risks or deal with issues that arise – continually benchmarked against expected parameters/tolerances

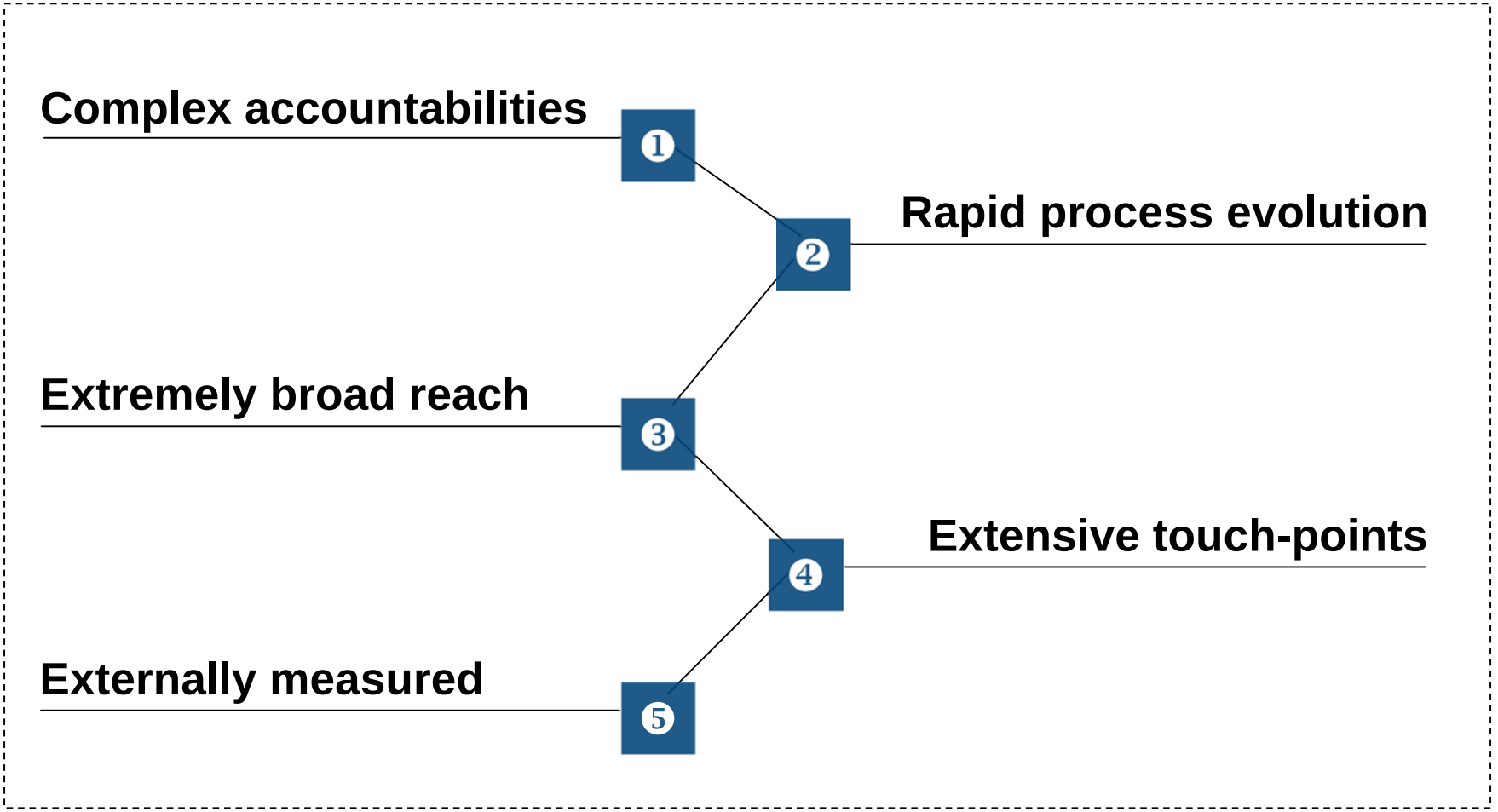
Starts with a Common Process Model

Critical components of an effective compliance program according to the US Sentencing Guidelines

Hypothesis – A Portfolio Strategy for GRC



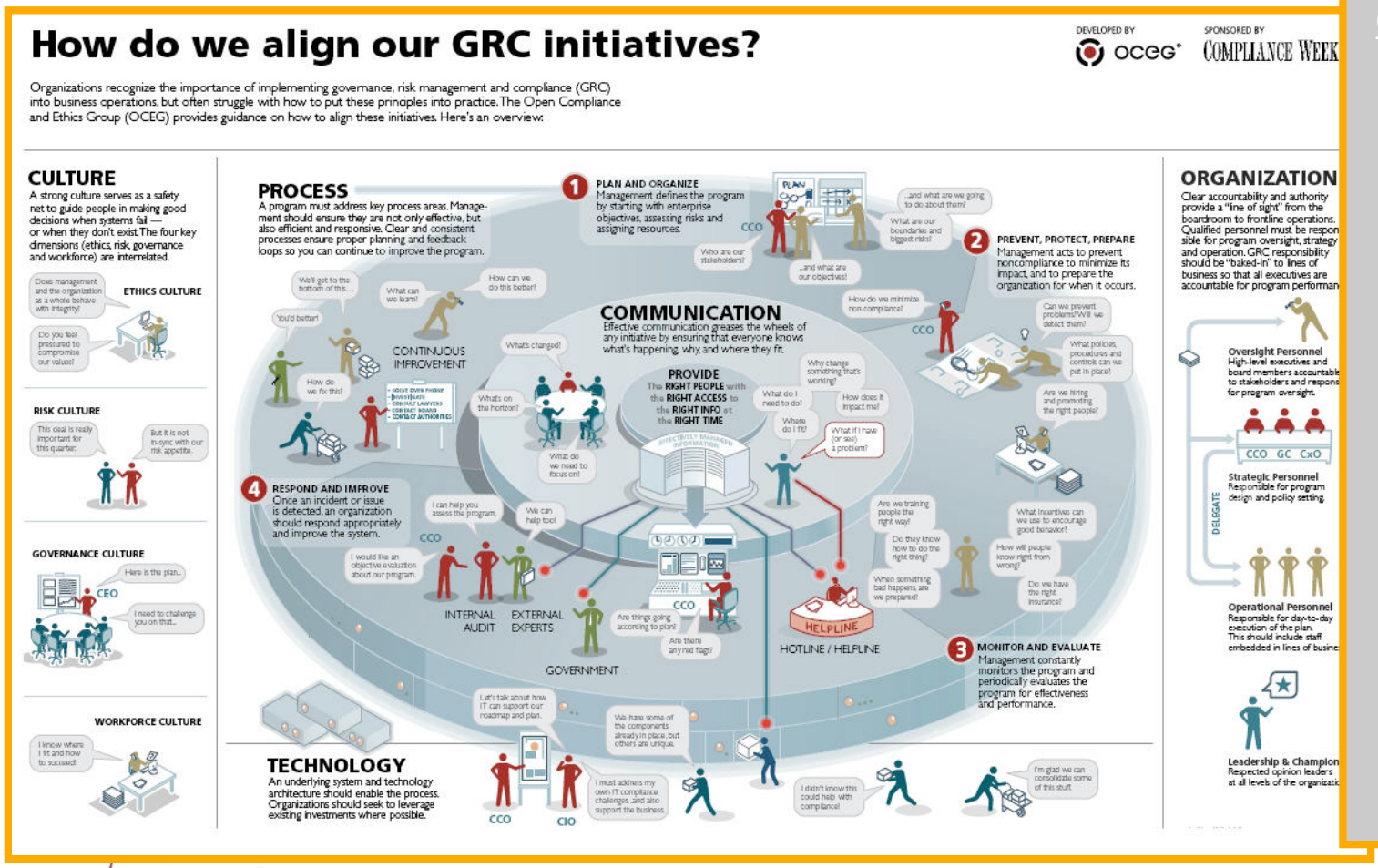
GRC A Complex Environment



But Common Process Yields Common Elements

√	**Process Activity**
	Track and assess legal requirements
	Manage and administer policies and procedures
	Periodically perform risk/impact assessments
	Monitor KCI's (key compliance indicators)
	Deploy training and monitor completions
	Maintain and execute audit plans
	Manage roles and responsibilities
	Incident and remediation management
	Periodic workforce and third-party surveys
	Change Management (people, processes, and technologies)
	Other Considerations
	Multiple operating units/LOB

OCEG Model Provides an Expanded GRC Vision



Small Sample of Members:

- ADM
- Dell
- Deloitte
- E&Y
- Freddie Mac
- Gevity
- Littler
- Marsh
- Petco
- PwC
- Quest
- Staples
- Wachovia
- WalMart
- Etc.

Question: What area presents the most challenge to achieving and sustaining Enterprise GRC?

Answers:

Organization - oversight team members, charter, team roles, execution team roles and responsibilities

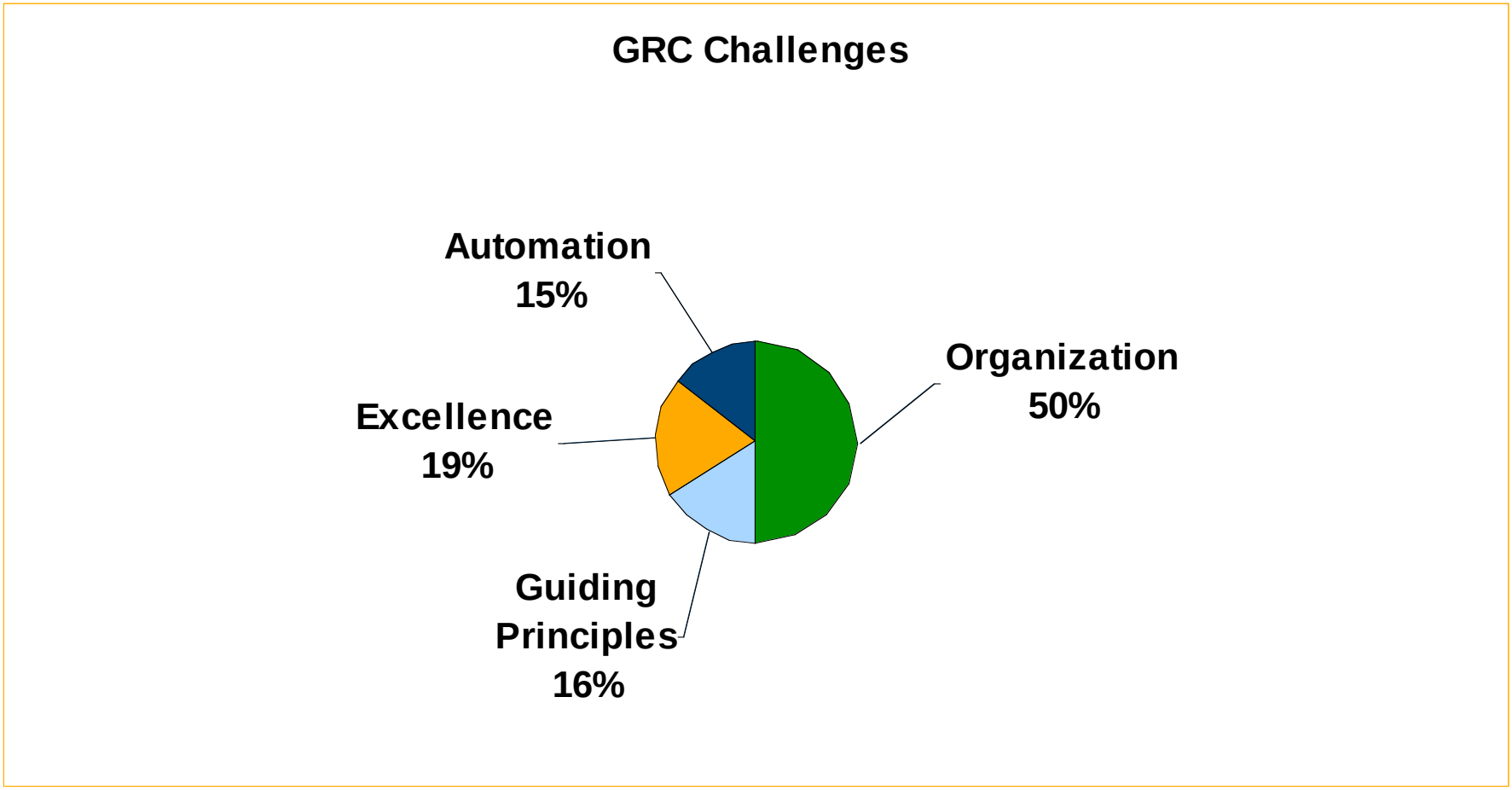
Guiding Principles – tone at the top, boundaries, expectations, culture, issue resolution

Automation – common technology architecture to support the common processes

Excellence - Consistent, Sustained, Available, Repeatable, Auditable, Effective, Efficient

All of the above

Results: What area presents the most challenge to achieving and sustaining Enterprise GRC?



GRC – Key Challenges and Scope of GRC

Enterprise Governance, Risk & Compliance

Key Challenges

- ***Organization*** - oversight team members, charter, team roles
- ***Guiding Principles*** – tone at the top, boundaries, expectations, culture
- ***Automation*** – reusable technology architecture to support the common processes
- ***Consistent, Sustained, Available, Repeatable, Auditable, Effective, Efficient***

Financial Risk Management	Operational Risk Management	Legal and Regulatory Risk Management	Strategic Risk Management
• Accounting practices	• Auditing and Monitoring	• Regulatory Compliance	• Corporate communications
• Capital structure	• IT Governance	• Ethics & Code of conduct	• Investor relations
• Credit availability	• People resources	• Litigation management	• M&A
• Taxes	• Business Relationships	• Corporate responsibility	• Divestiture
• Liquidity	• Physical assets		• Brand & reputation
	• Sales & Marketing		• Competition
	• Health & Safety		• Market volatility
	• Fraud		
	• Complaint Handling		

Broad Technology Requirements ….

- Purpose built for organizing GRC
- Ease of administration and maintenance
- Ability to execute process elements across domains
- Individual process visibility and measurement
- Cross-process visibility and measurement
- Easy extension to trading partners, vendors
- Extensive integration with various systems
- System adaptability to meet changing needs

… Drive Specific Technical Considerations

Complex accountabilities

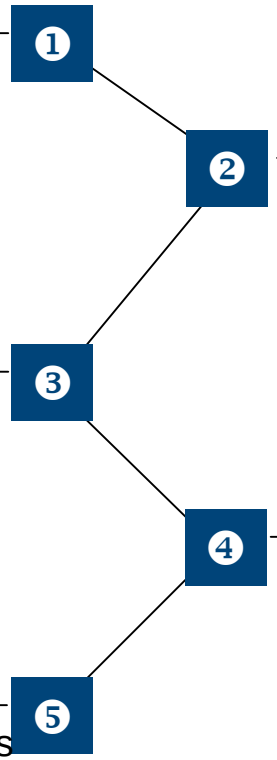
- Complex groupings
- Decentralized administration
- Robust security
- Sophisticated, flexible reporting

Extremely broad reach

- Substantial volume/scalability
- Worldwide reach (zero footprint)
- Simplicity/consistency (no training)
- Low average cost per user

Externally measured

- Auditors, regulators, prosecutors, courts
- Investors, financial institutions & markets
- Customers, partners



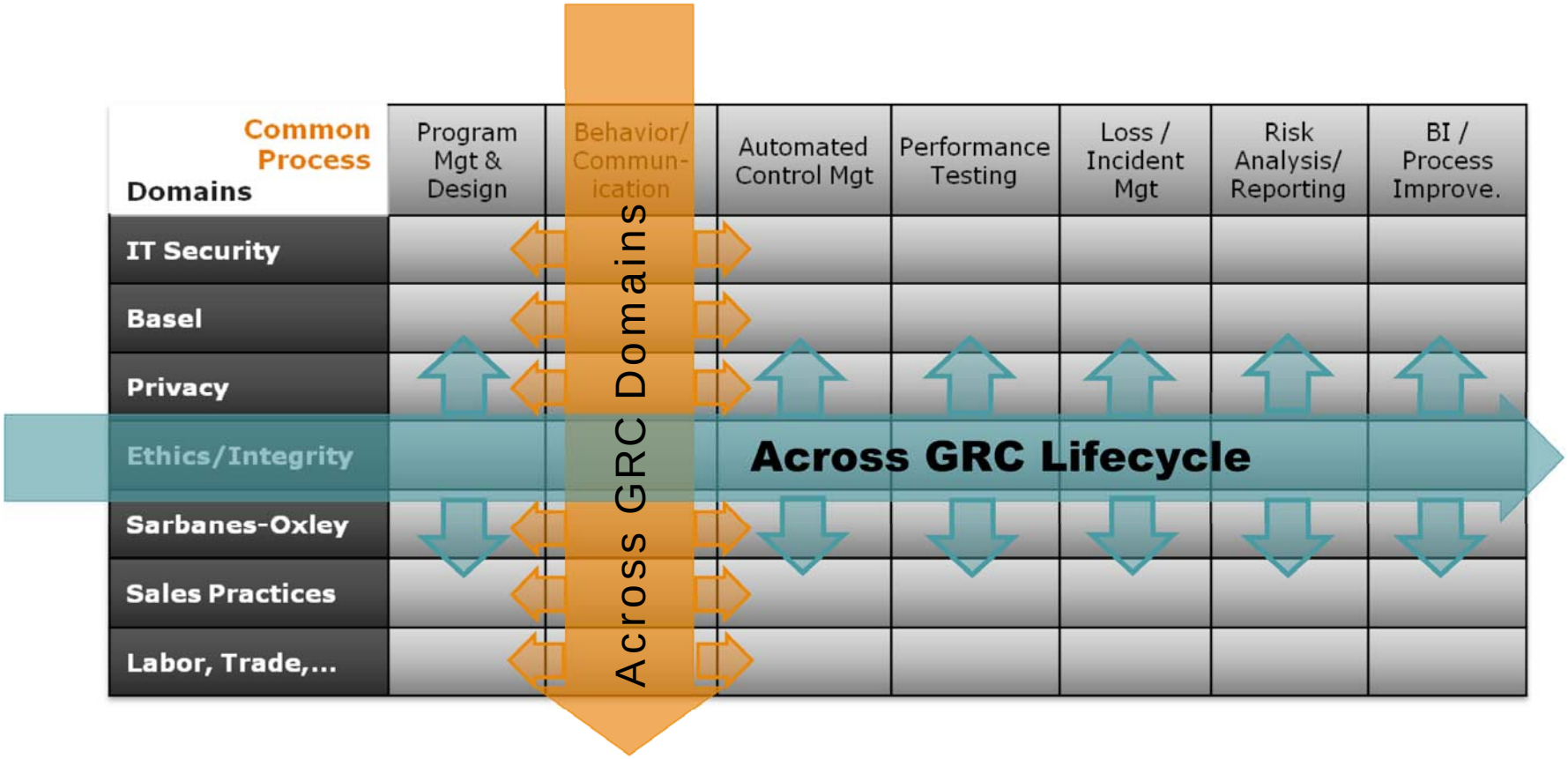
Rapid process evolution

- Rapid application enhancement
- Material application flexibility
- Integrated change management
- Comprehensive audit trail

Extensive touch-points

- ERP/HRIS integration
- Strong application integration capabilities and strategy
- System control identification and integration

GRC Starting Points – Think Big, Implement Small



Question: What is most difficult area to address in building your business case?

Answers:

a) Cross organizational impacts – resources, politics, personal agendas, buy-in

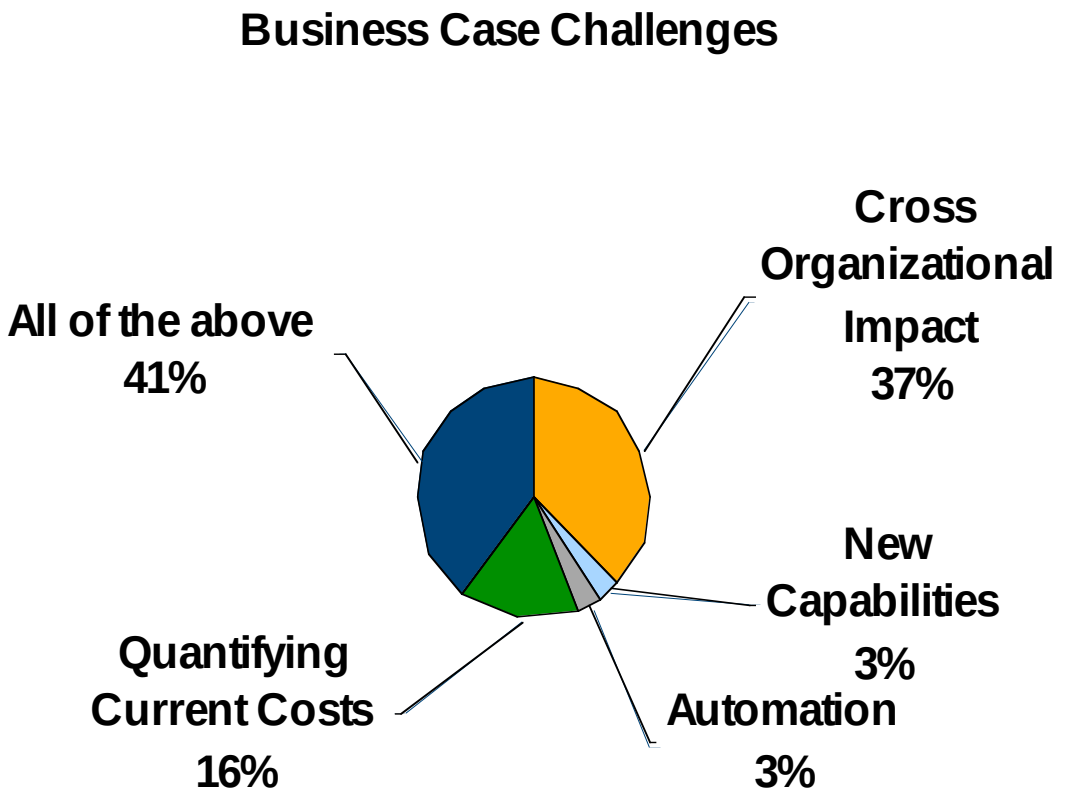
b) New capabilities – Little prior experience with forecasting the impact of new capabilities

c) Automation – forecasting other uses beyond initial catalyst, replacement/consolidation of existing technology

d) Quantifying current costs – no actual cost to compare against new capabilities, processes, and functions

e) All of the above

Results: What is most difficult area to address in building your business case?



GRC Business Case

- **Requirement and Cost Matrix:**
  - Key process functions (execution and oversight)
  - FTE's, Technology (initial, ongoing)
  - Options and Recommendations

- **Other Considerations:**
  - Cost of status-quo (risk tolerance, resources, technology and expenses)
  - Ability to leverage existing capabilities (resources and technology)
  - New approach (simplification, consolidation, increased opportunities, rapid benefits, long term solution)

GRC Can Generate Strong ROI

Results from a recent "Total Economic Impact" study performed by Forrester.

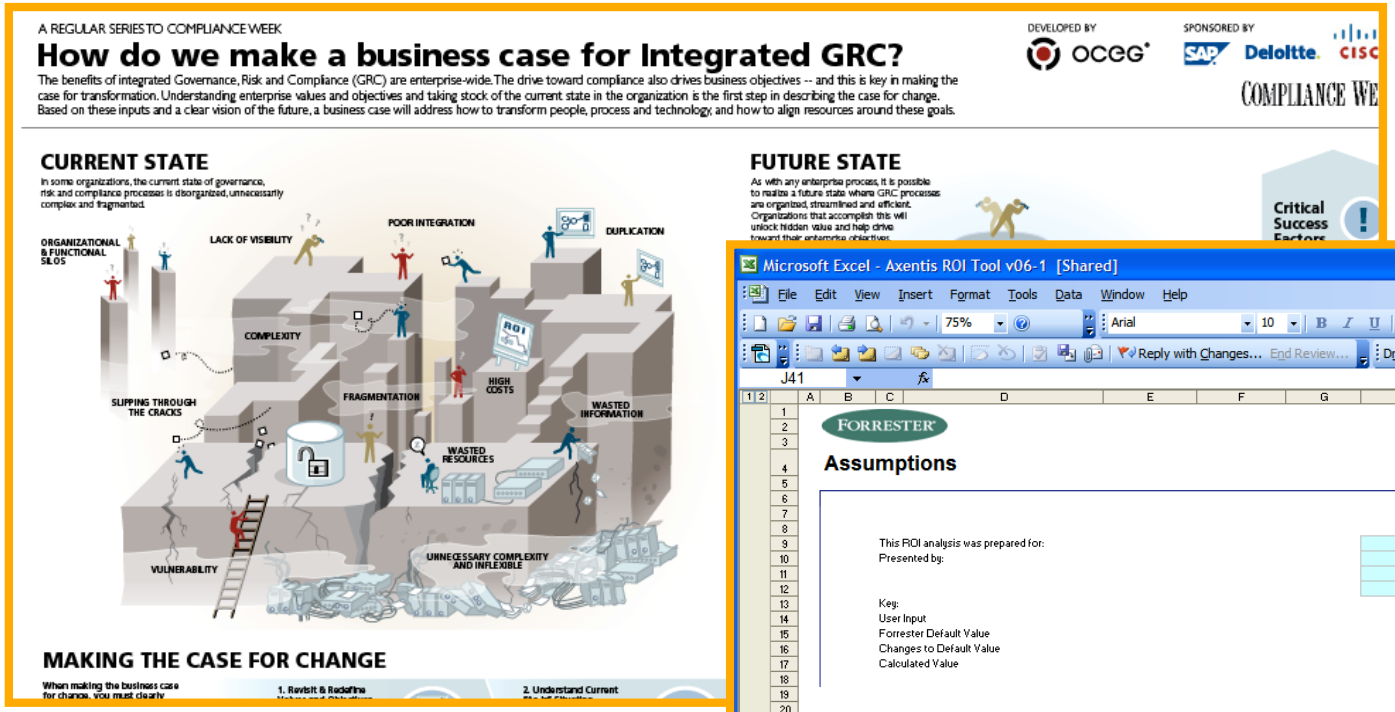
Cash Flow	*Initial Cost*	*Year 1*	*Year 2*	*Year 3*	*Year 4*	*Year 5*	*Total*	*Present Value*
Total Costs	10,880	510,970	696,218	458,428	504,816	404,500	2,585,812	1,991,168
Total Benefits		558,807	1,610,993	1,633,793	1,955,393	1,981,793	7,740,779	5,632,995
Total	10,880	47,837	914,775	1,175,365	1,450,577	1,577,293	5,154,967	3,641,827

GRC requires a shift in mindset to adopt a new approach supported by appropriately applied technology.

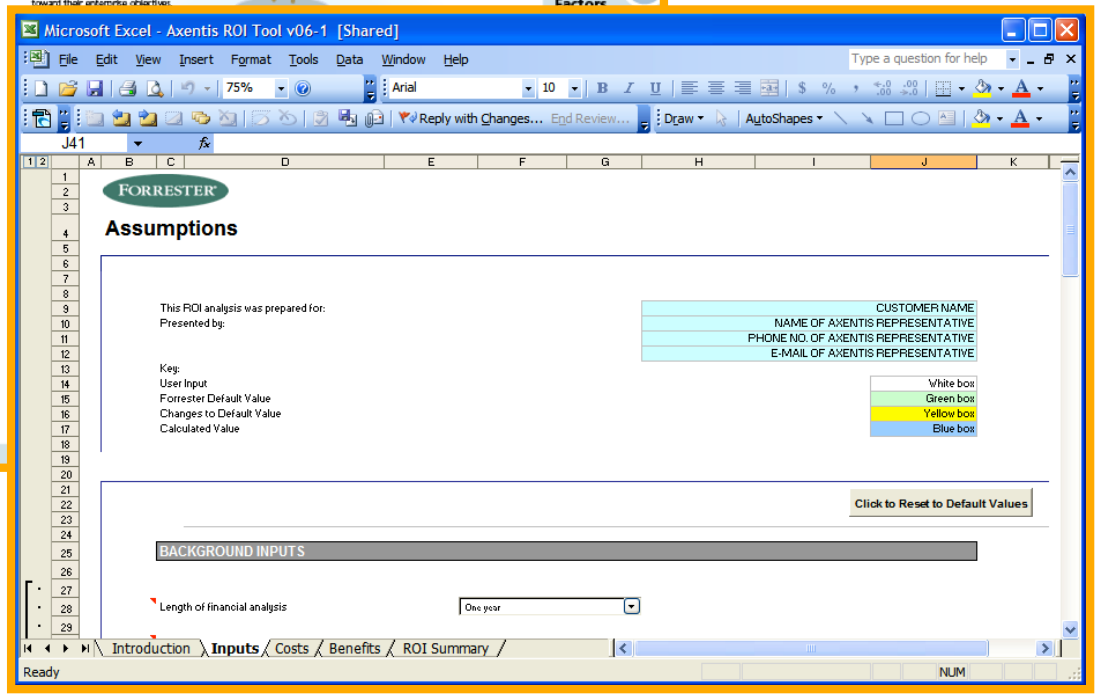
Disclaimer: Read full report for details, individual results may vary

Business Case Resources

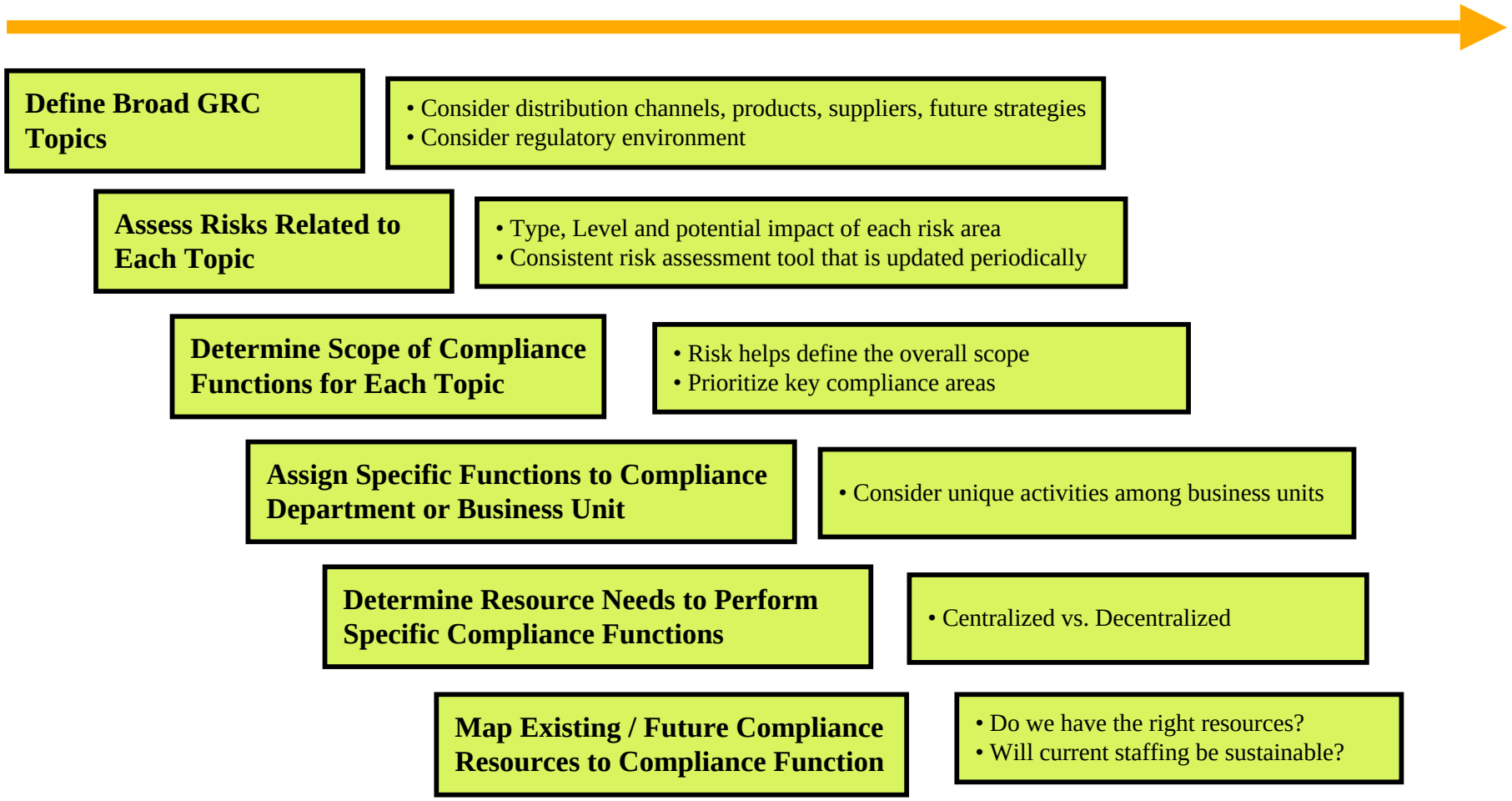
OCEG



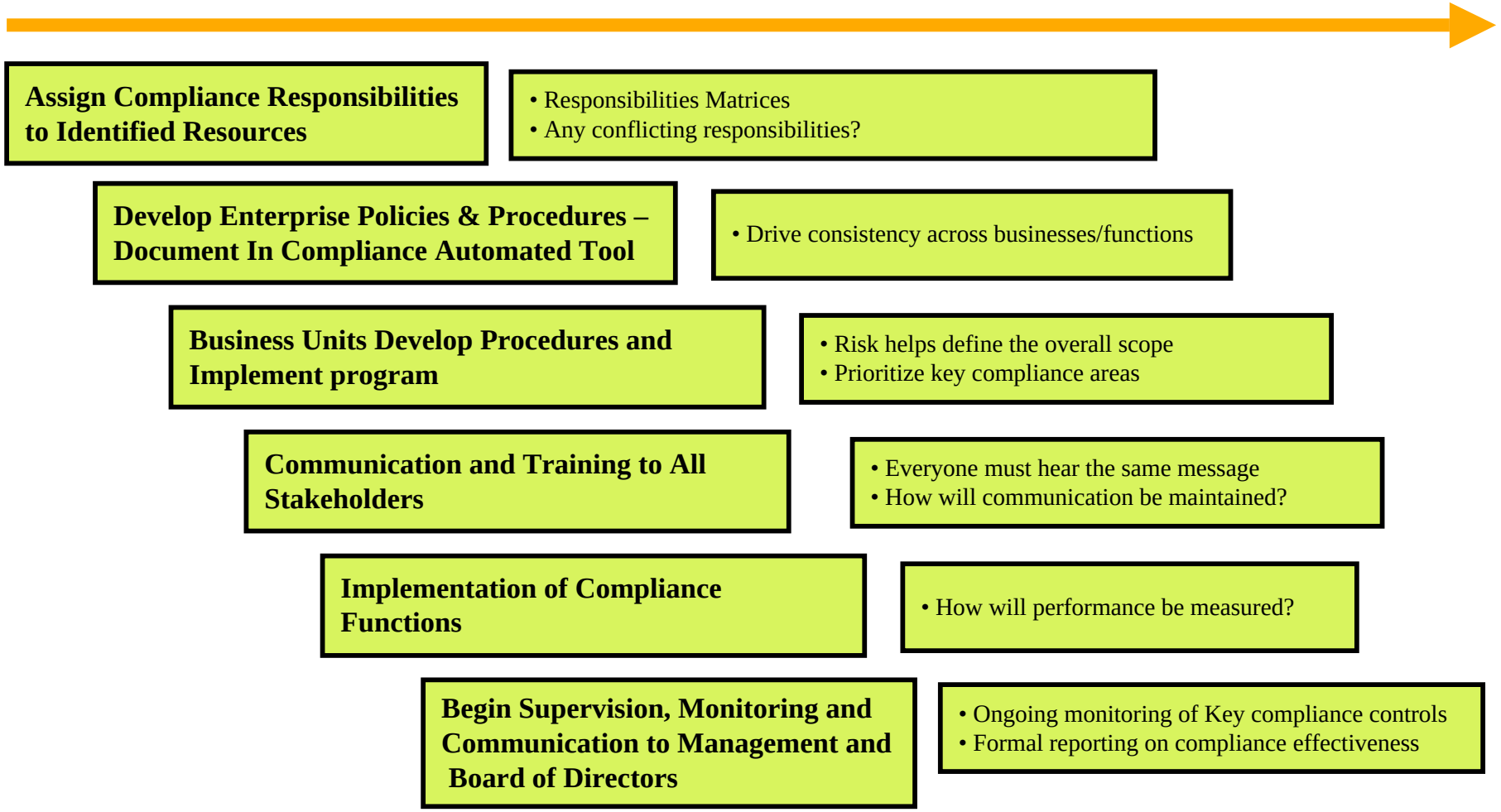
Forrester



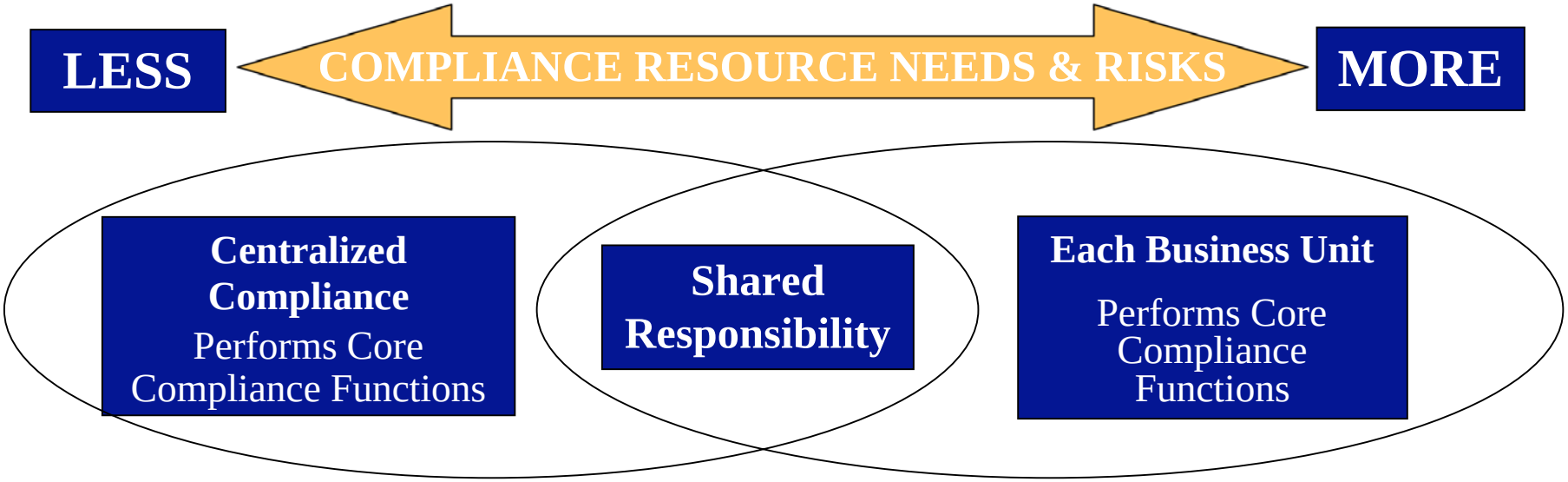
Design Strategy – Phase I



Implementation Strategy – Phase II



GRC Responsibility Considerations



Where the Majority of Core Compliance Functions for Various Compliance Topics Are Generally Handled In A Matrix Structured Compliance Operation

Compliant Handling **Sales Practice Monitoring** **AML/OFAC** **Advertising and Sales Material Review**

HR **Compliance Risk Assessment**

Training

Recruiting, Licensing & Appointment **Do-Not-Call/CAN Spam** **Corporate Governance** **Ethics**

HIPAA **TPA Monitoring** **Filings** **SOX**

Key Drivers of Successful Implementations

- ✓ Organization, planning and execution – “Tone at the top”
- ✓ Executive sponsorship and support
  - – Program management level planning
  - – Plan execution and preparing the business community
- ✓ Internal implementation team
  - – Availability of key players, accountability, authority
- ✓ Technology
  - – Support the initial needs with room to grow
- ✓ Partner implementation team
  - – Experienced, focused, committed to your success
- ✓ Think about the bigger vision, strategy and plan
  - – Execute the task at hand

Question and Answer

Thank you,

Brett Curran

bcurran@axentis.com