



Integrated Governance, Risk and Compliance

Brett Curran

Director GRC Practices - Axentis

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:

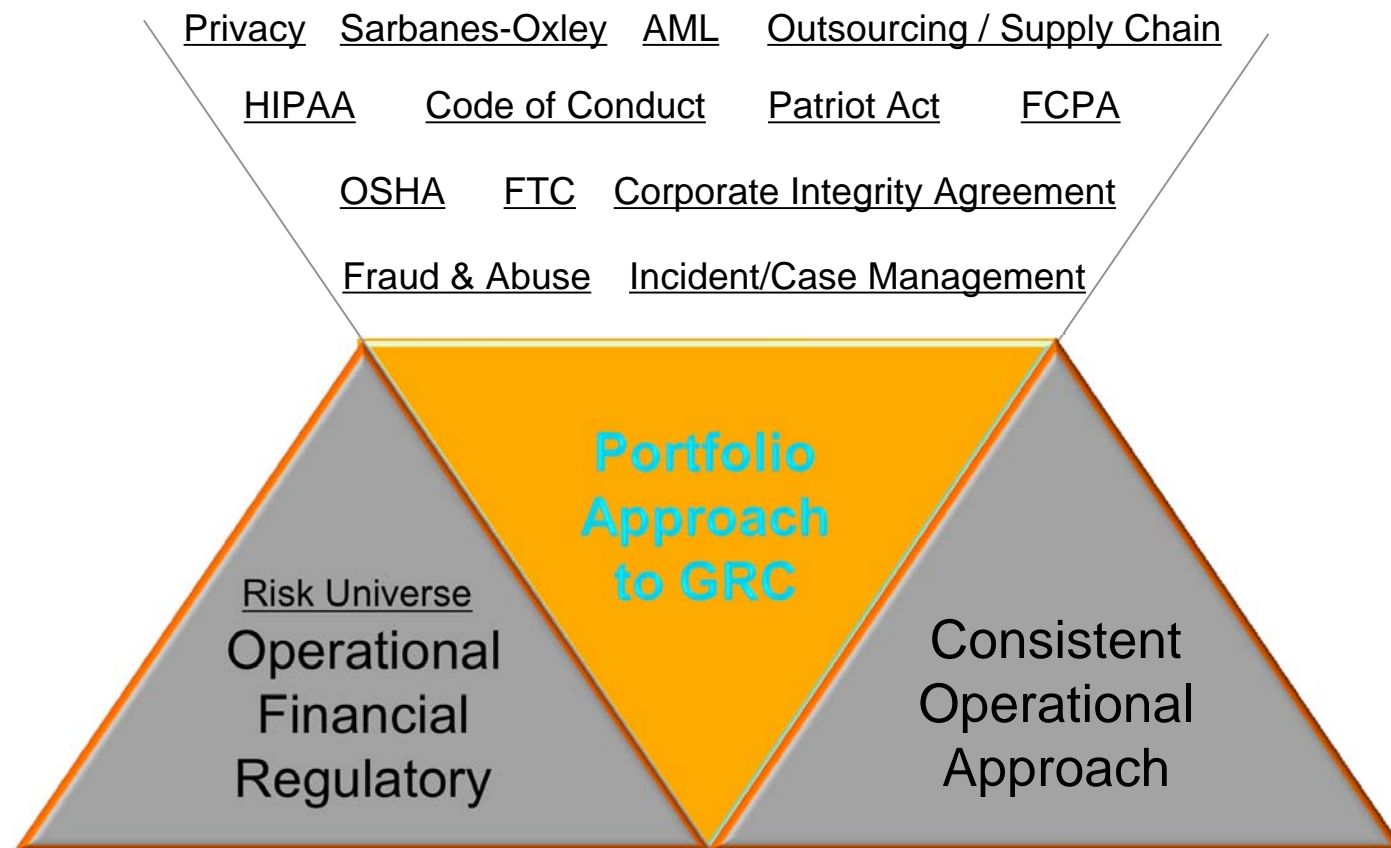
- Execution of business processes designed to control/manage risks or deal with issues that arise – continually benchmarked against expected parameters/tolerances

Starts with a Common Process Model

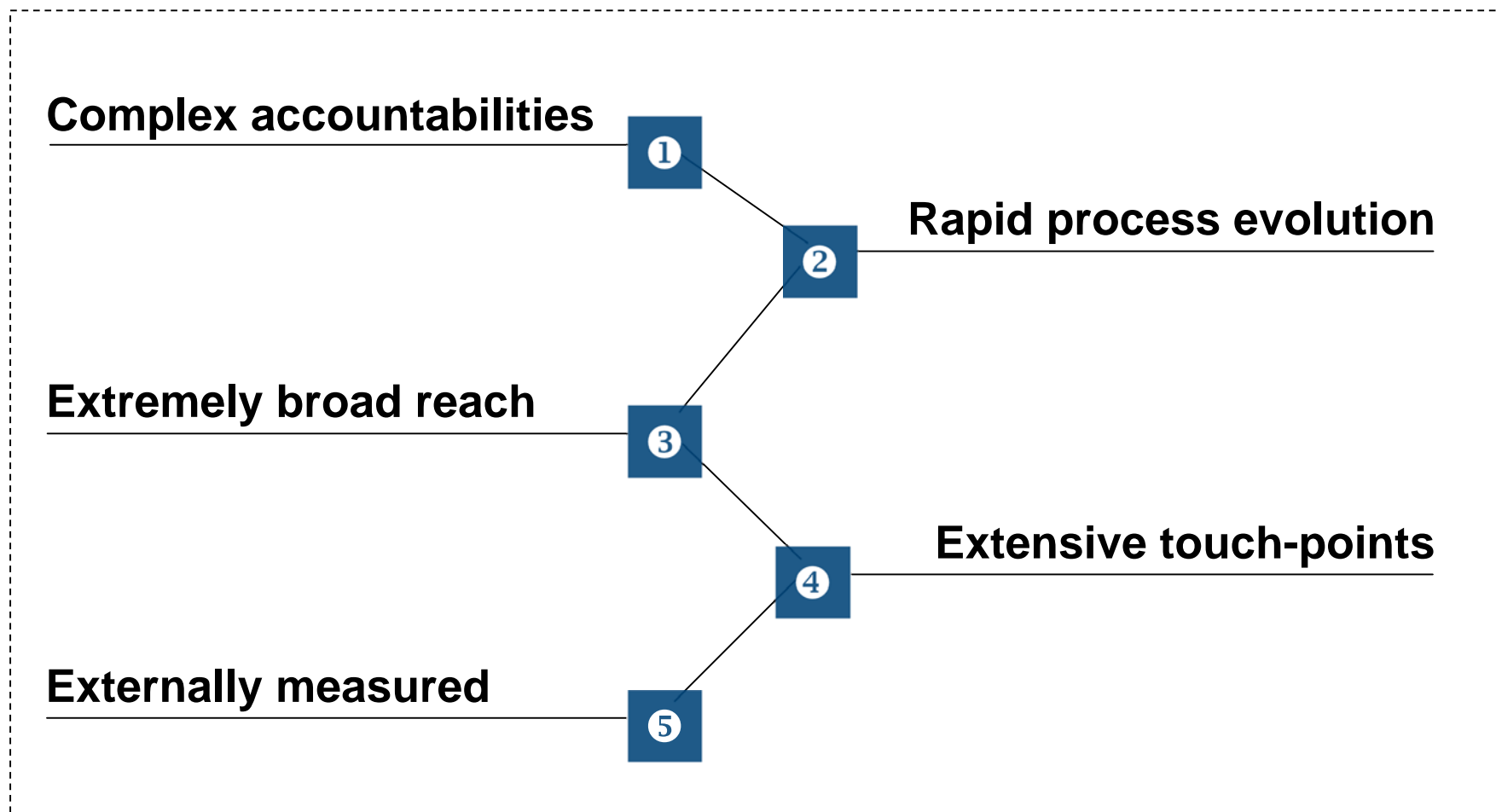


Critical components of an effective compliance program according to the US Sentencing Guidelines

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

How do we align our GRC initiatives?

Organizations recognize the importance of implementing governance, risk management and compliance (GRC) into business operations, but often struggle with how to put these principles into practice. The Open Compliance and Ethics Group (OCEG) provides guidance on how to align these initiatives. Here's an overview.

DEVELOPED BY
OCEG
SPONSORED BY
COMPLIANCE WEEK

CULTURE

A strong culture serves as a safety net to guide people in making good decisions when systems fail — or when they don't exist. The four key dimensions (ethics, risk, governance and workforce) are interrelated.

ETHICS CULTURE
Does management and the organization as a whole behave with integrity?
Do you feel pressured to compromise your values?

RISK CULTURE

This deal is really important for this quarter.
But it is not in sync with our risk appetite.

GOVERNANCE CULTURE

Here is the plan...
I need to challenge you on that...

WORKFORCE CULTURE

I know where I fit and how to succeed.

PROCESS

A program must address key process areas. Management should ensure they are not only effective, but also efficient and responsive. Clear and consistent processes ensure proper planning and feedback loops so you can continue to improve the program.

CONTINUOUS IMPROVEMENT
We'll get to the bottom of this...
What can we learn?
How can we do this better?
You'd better!
How do we fix this?

4 RESPOND AND IMPROVE
Once an incident or issue is detected, an organization should respond appropriately and improve the system.

I can help you assess the program.
We can help too!

I would like an objective evaluation about our program.

INTERNAL AUDIT
EXTERNAL EXPERTS

GOVERNMENT

Let's talk about how IT can support our roadmap and plan.

We have some of the components already in place, but others are unique.

I must address my own IT compliance challenges, and also support the business.

CCO CIO

TECHNOLOGY
An underlying system and technology architecture should enable the process. Organizations seek to leverage existing investments where possible.

1 PLAN AND ORGANIZE
Management defines the program by starting with enterprise objectives, assessing risks and assigning resources.

Who are our stakeholders?
What are our objectives?
What are our boundaries and biggest risks?
How do we minimize non-compliance?

Can we prevent problems? Will we detect them?
What policies, procedures and controls can we put in place?
Are we hiring and promoting the right people?

Are we training people the right way?
Do they know how to do the right thing?
When something bad happens are we prepared?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

2 PREVENT, PROTECT, PREPARE
Management acts to prevent non-compliance to minimize its impact, and to prepare the organization for when it occurs.

Who are our stakeholders?
What are our objectives?
What are our boundaries and biggest risks?
How do we minimize non-compliance?

Can we prevent problems? Will we detect them?
What policies, procedures and controls can we put in place?
Are we hiring and promoting the right people?

Are we training people the right way?
Do they know how to do the right thing?
When something bad happens are we prepared?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

3 MONITOR AND EVALUATE
Management constantly monitors the program and periodically evaluates the program for effectiveness and performance.

Who are our stakeholders?
What are our objectives?
What are our boundaries and biggest risks?
How do we minimize non-compliance?

Can we prevent problems? Will we detect them?
What policies, procedures and controls can we put in place?
Are we hiring and promoting the right people?

Are we training people the right way?
Do they know how to do the right thing?
When something bad happens are we prepared?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

What do I have (or see) a problem?
What do I need to do?
How does it impact me?

ORGANIZATION

Clear accountability and authority provide a "line of sight" from the boardroom to frontline operations. Qualified personnel must be responsible for program oversight, strategy and operation. GRC responsibility should be "baked-in" to lines of business so that all executives are accountable for program performance.

Oversight Personnel
High-level executives and board members accountable to stakeholders and responsible for program oversight.

Strategic Personnel
Responsible for program design and policy setting.

Operational Personnel
Responsible for day-to-day execution of the plan. This should include staff embedded in lines of business.

Leadership & Champion
Respected opinion leaders at all levels of the organization.

Small Sample of Members:

ADM
Dell
Deloitte
E&Y
Freddie Mac
Geivity
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

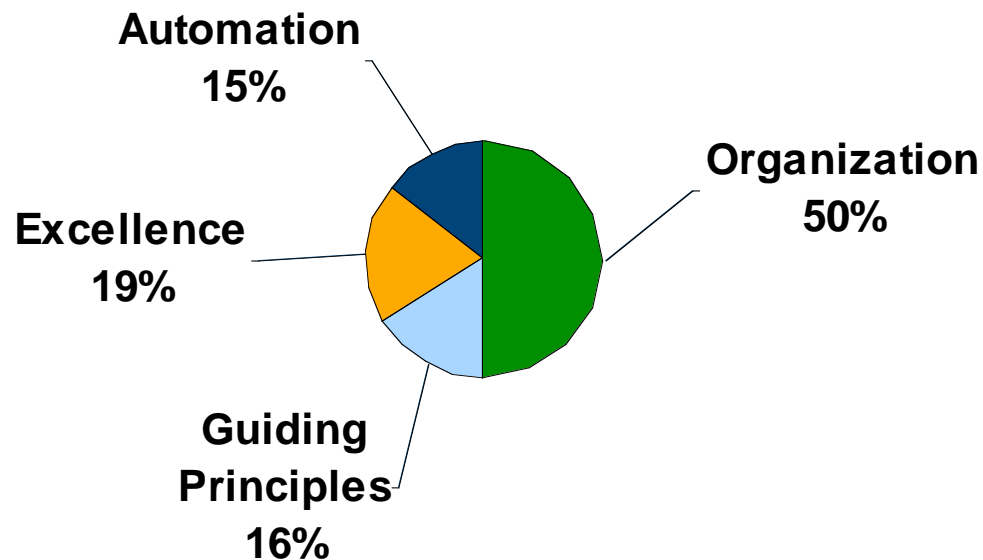
Automation – common technology architecture to support the common processes

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 Challenges



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

- Accounting practices
- Capital structure
- Credit availability
- Taxes
- Liquidity

Operational Risk Management

- Auditing and Monitoring
- IT Governance
- People resources
- Business Relationships
- Physical assets
- Sales & Marketing
- Health & Safety
- Fraud
- Complaint Handling

Legal and Regulatory Risk Management

- Regulatory Compliance
- Ethics & Code of conduct
- Litigation management
- Corporate responsibility

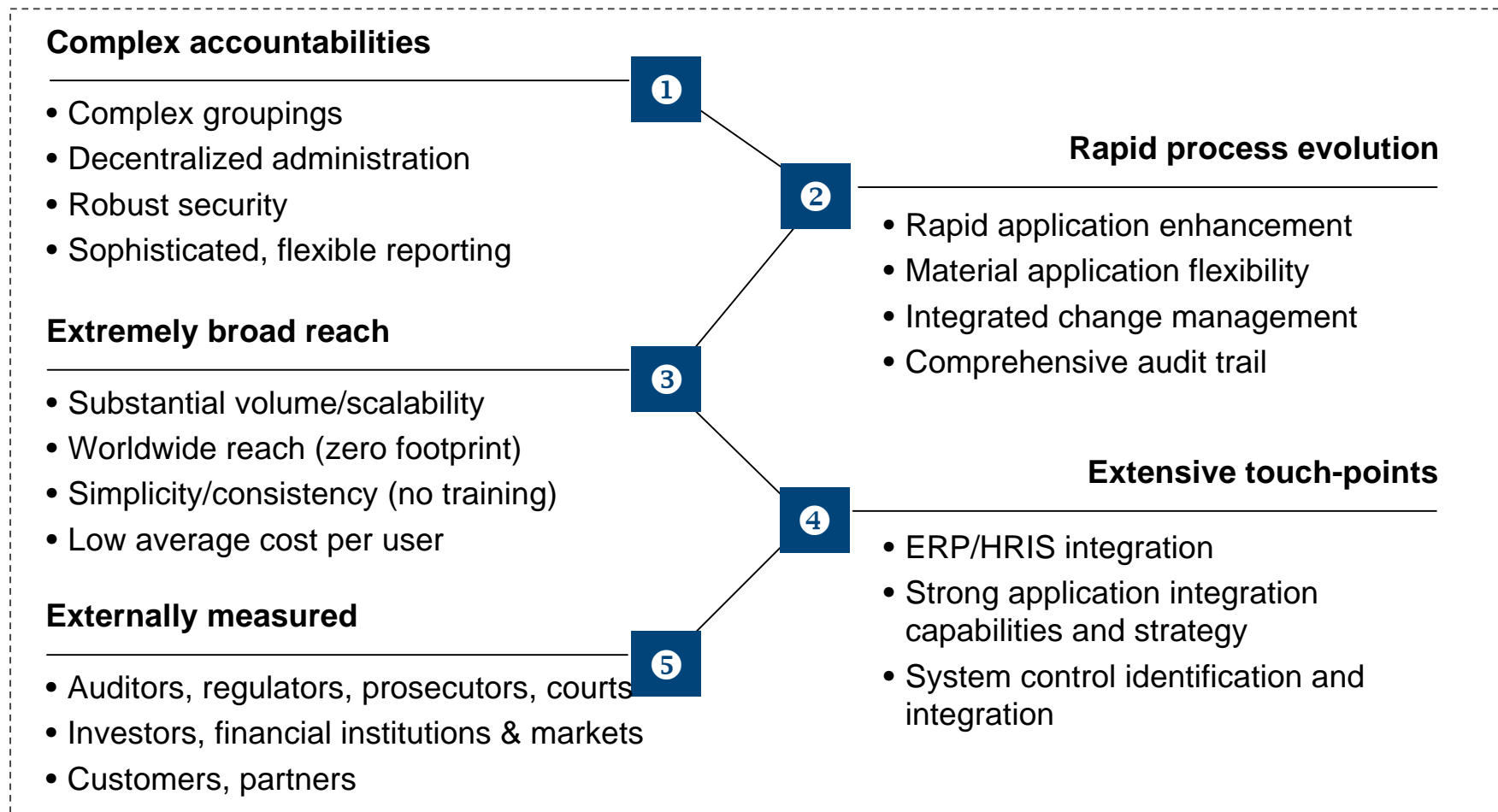
Strategic Risk Management

- Corporate communications
- Investor relations
- M&A
- Divestiture
- Brand & reputation
- Competition
- Market volatility

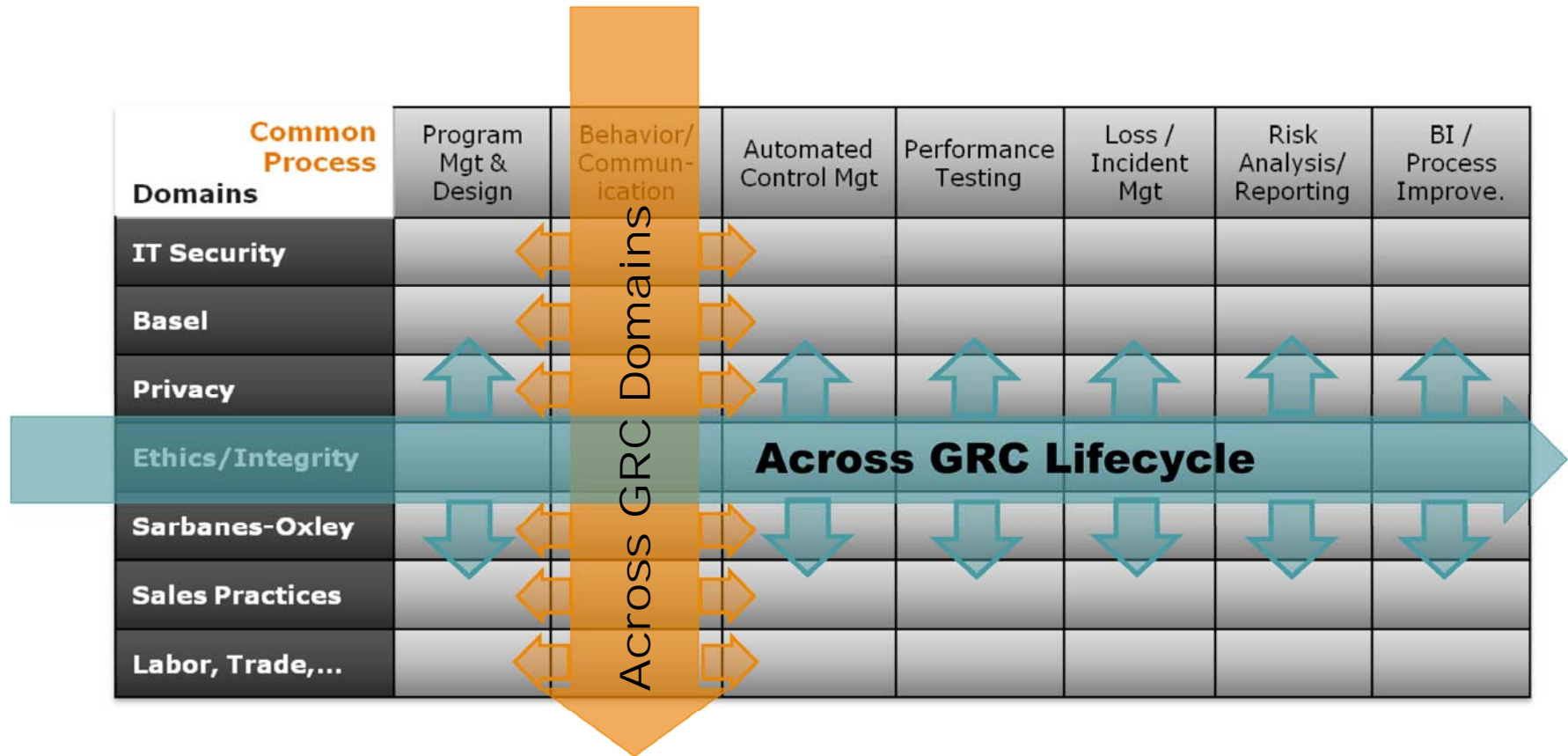
Broad Technology Requirements

- 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



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

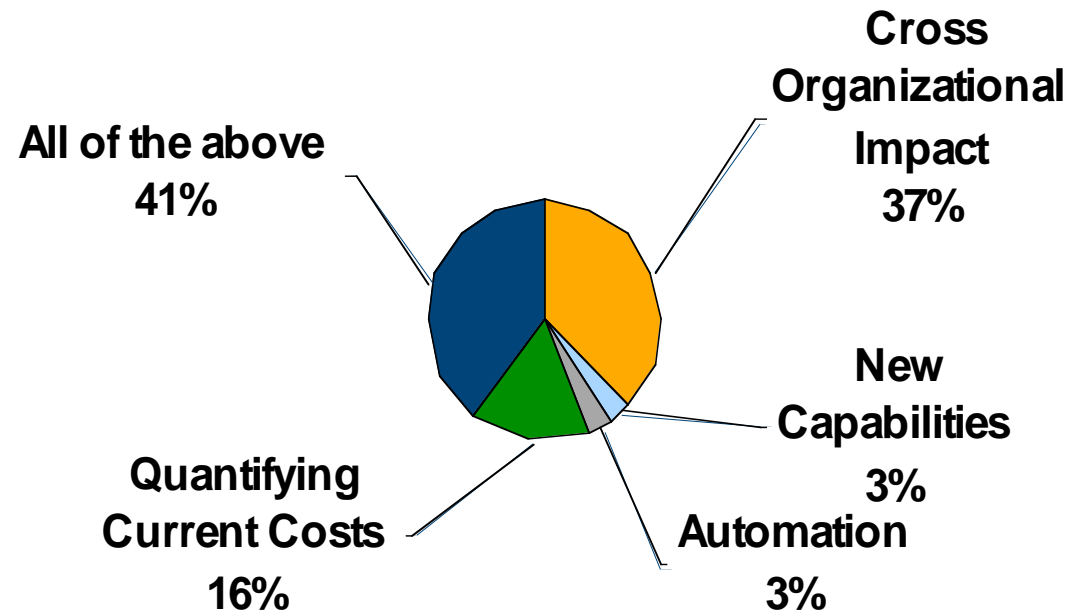
c) *Automation* – forecasting other uses beyond initial catalyst, replacement/consolidation of existing technology

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?

Business Case Challenges



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.



<i>Cash Flow</i>	<i>Initial Cost</i>	<i>Year 1</i>	<i>Year 2</i>	<i>Year 3</i>	<i>Year 4</i>	<i>Year 5</i>	<i>Total</i>	<i>Present Value</i>
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

A REGULAR SERIES TO COMPLIANCE WEEK

How do we make a business case for Integrated GRC?

The benefits of integrated Governance, Risk and Compliance (GRC) are enterprise-wide. The drive toward compliance also drives business objectives -- and this is key in making the case for transformation. Understanding enterprise values and objectives and taking stock of the current state in the organization is the first step in describing the case for change. Based on these inputs and a clear vision of the future, a business case will address how to transform people, process and technology; and how to align resources around these goals.

DEVELOPED BY oceg[®] **SPONSORED BY** SAP Deloitte cisco

CURRENT STATE
In some organizations, the current state of governance, risk and compliance processes is disorganized, unnecessarily complex and fragmented.

FUTURE STATE
As with any enterprise process, it is possible to realize a future state where GRC processes are organized, streamlined and efficient. Organizations that accomplish this will unlock hidden value and help drive forward their enterprise objectives.

COMPLIANCE WEEK

Forrester

MAKING THE CASE FOR CHANGE
When making the business case for change, you must clearly:

1. Revisit & Redefine
2. Understand Current

Microsoft Excel - Axiomis ROI Tool v06-1 [Shared]

File Edit View Insert Format Tools Data Window Help

Type a question for help

75% Arial 10

Draw AutoShapes

J41

FORRESTER

Assumptions

This ROI analysis was prepared for:
Presented by:

Key:
User Input
Forrester Default Value
Changes to Default Value
Calculated Value

CUSTOMER NAME
NAME OF AXIOMIS REPRESENTATIVE
PHONE NO. OF AXIOMIS REPRESENTATIVE
E-MAIL OF AXIOMIS REPRESENTATIVE

White box
Green box
Yellow box
Blue box

Click to Reset to Default Values

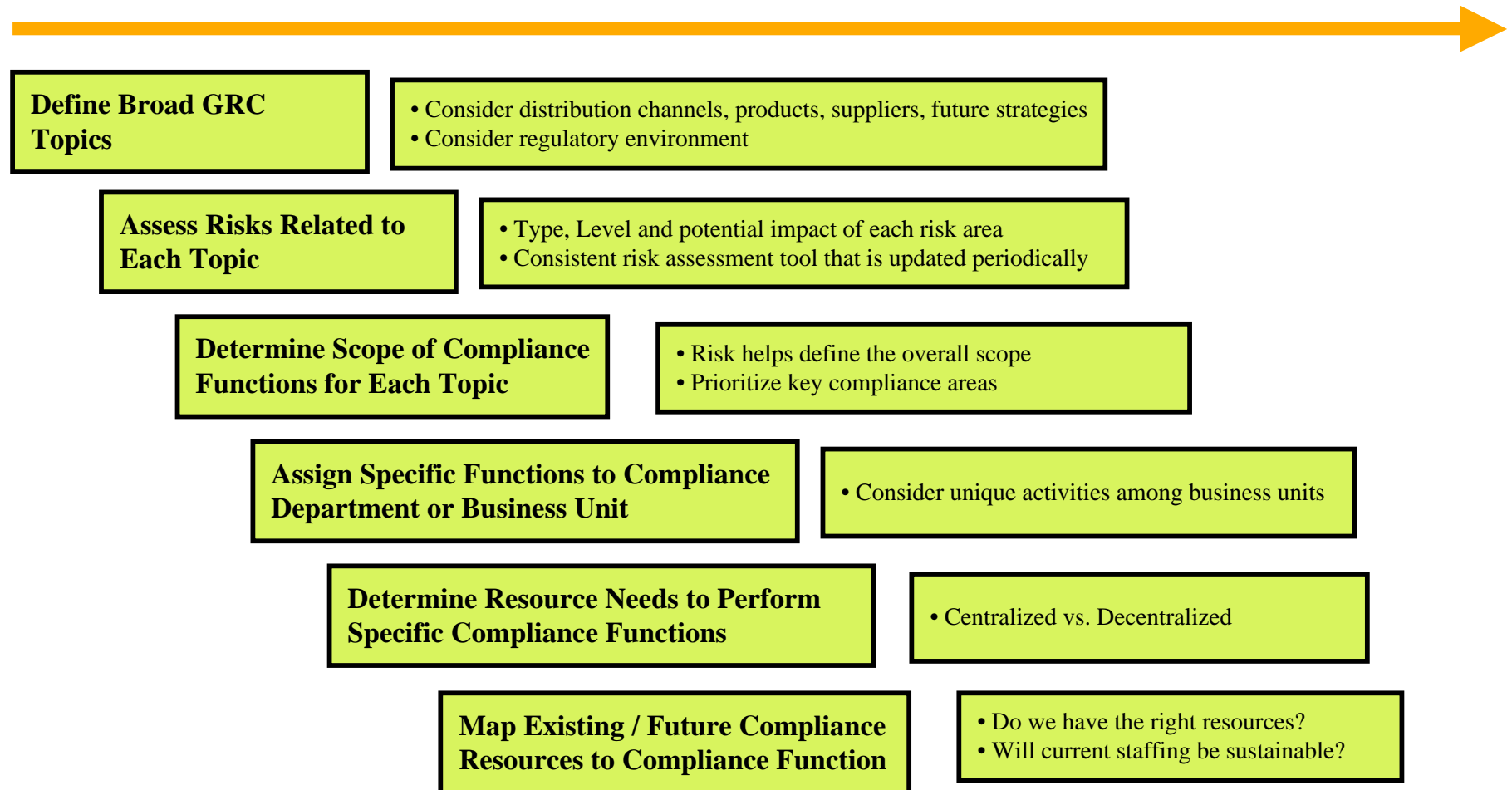
BACKGROUND INPUTS

Length of financial analysis One year

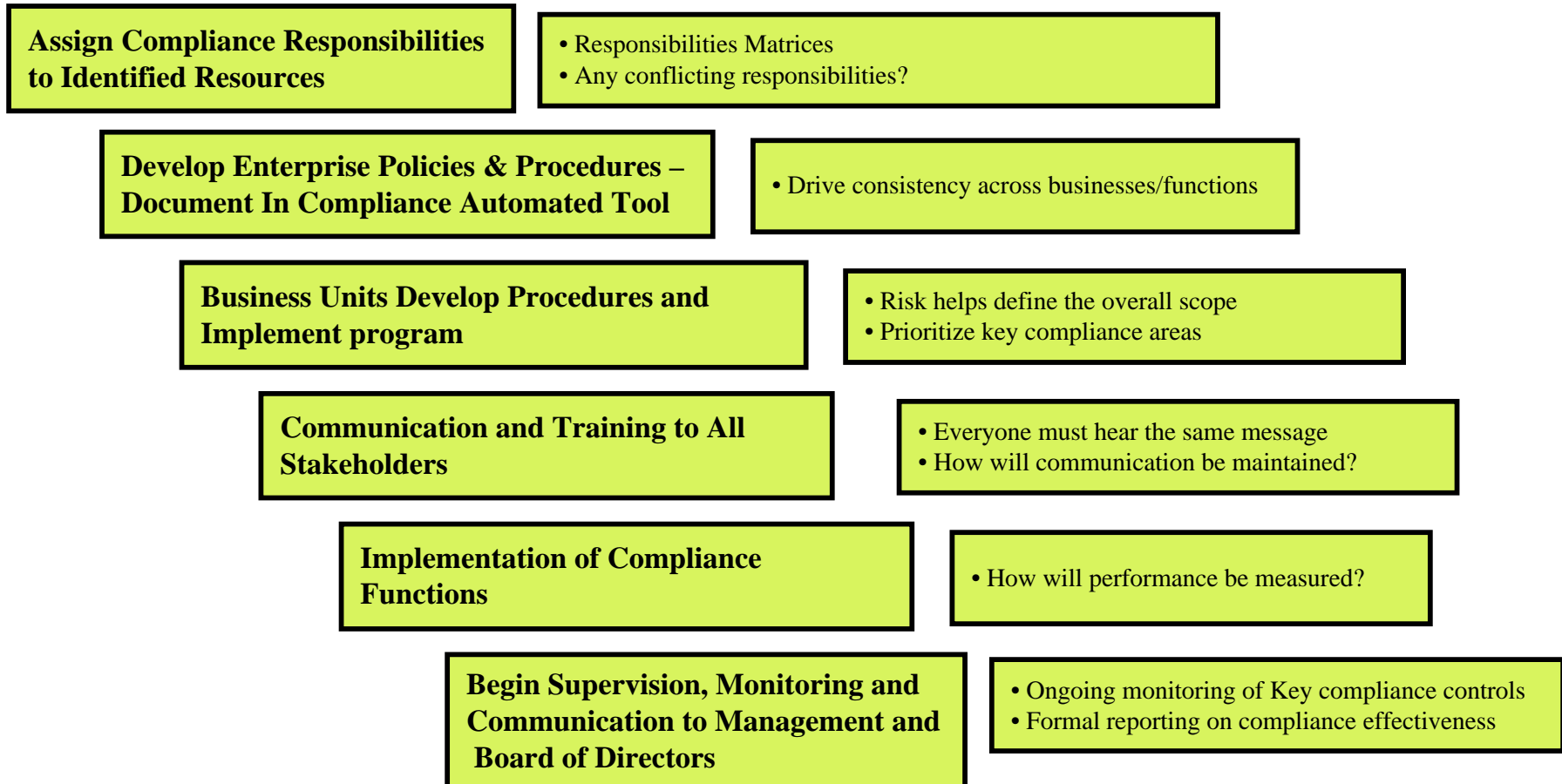
Introduction Inputs Costs Benefits ROI Summary

Ready NUM

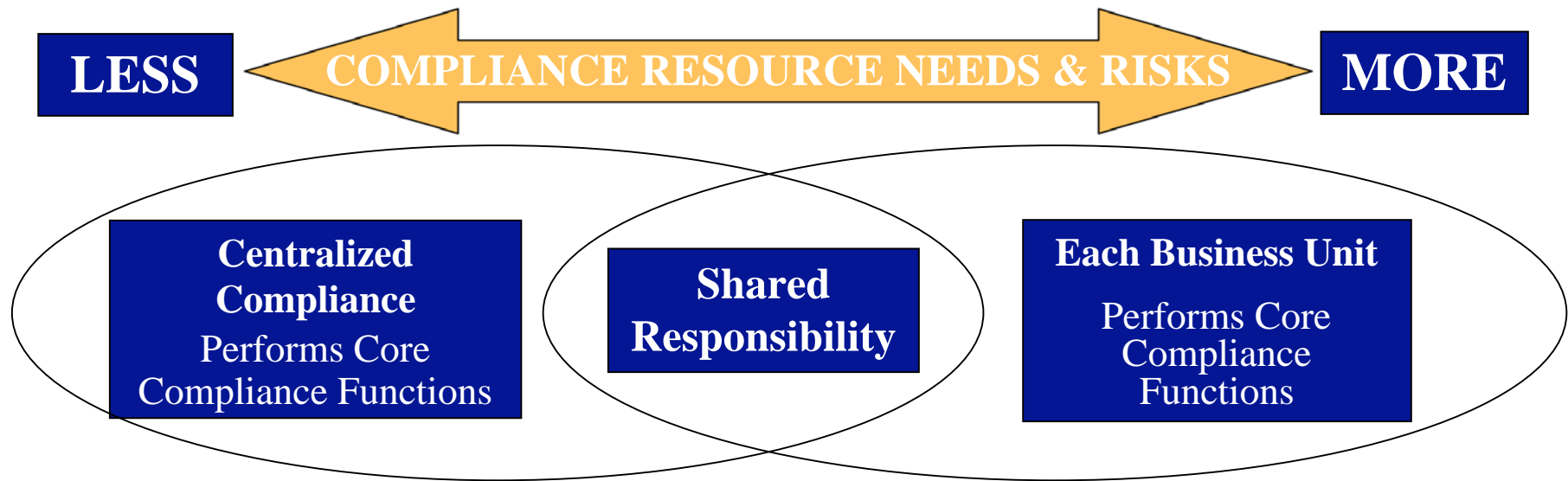
Design Strategy – Phase I



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	AML/OFAC	Advertising and Sales Material Review	
HR	Monitoring		Compliance Risk Assessment	
Recruiting, Licensing & Appointment	Training	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