Enhancing Enterprise Risk Management through GRC

Debbie Seidel

March 4, 2015

T. Rowe Price

- *We are an independent investment management firm with an unwavering focus on helping investors around the world achieve their long-term goals*

- Manage $747B in assets globally for a diversified client base across four primary distribution channels:
  - Third-party financial intermediaries that distribute our managed investment portfolios in the U.S. and other countries
  - Individual U.S. investors on a direct basis
  - U.S. defined contribution retirement plans
  - Institutional investors globally

- Over 5,870 associates located across 14 countries

- RSA Archer eGRC Background:
  - Client since 2010 using: Enterprise, Risk Management, Compliance, Vendor, Business Continuity and Policy
  - Initial purchase was by our Vendor Management group to facilitate Security Assessments
  - Implemented various capabilities between 2010-2014, such as Sarbanes Oxley Compliance, Business Continuity
  - All approached as independent, non-integrated projects…until we went to implement Enterprise Risk Management on the platform

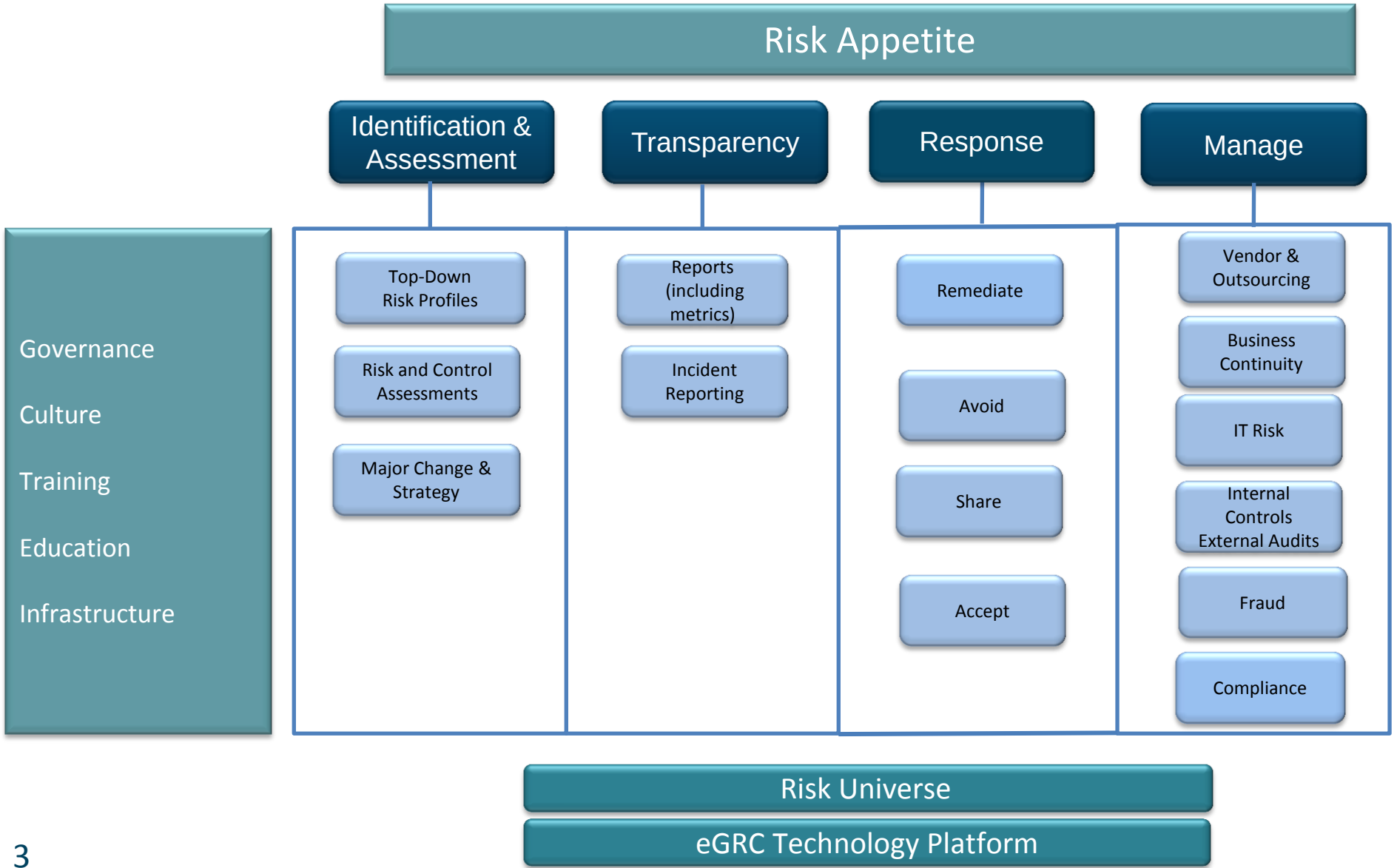
- Current Initiatives:
  - We are working with a consultant to assess the current state and how to evolve to support a GRC Strategy

Objectives Today

Discuss how an effective Governance, Risk and Compliance (GRC) strategy with integrated technology is a key component to Enterprise Risk Management

- Background on T. Rowe Price's Enterprise Risk Management
- Why we are pursuing a GRC Strategy
- Where we are going
- Lessons Learned

T. Rowe Price Enterprise Risk Management Framework Components



Enterprise Risk Management is across three lines of defense

To meet the challenges confronting a global organization, an Enterprise Risk Management Program is designed with lines of defense to identify, assess and manage risk.

Preparing the first line of defense (business managers and associates) with the knowledge, skills and capabilities is proactive risk management

All lines need to adopt a common approach (processes, taxonomy, etc.) to support the first line of defense

Integrated risk management is a necessity for T. Rowe Price as our business grows more complex and we continue to manage external volatility

Internal drivers

- T. Rowe's business model is becoming increasingly more complex (product, distribution, outsourcing/offsite processing)
- Business Units are expected to perform more risk and compliance activities without necessarily having the knowledge, skills or abilities
- A strategic view of risk is increasingly important to understand the impact across various channels

External drivers

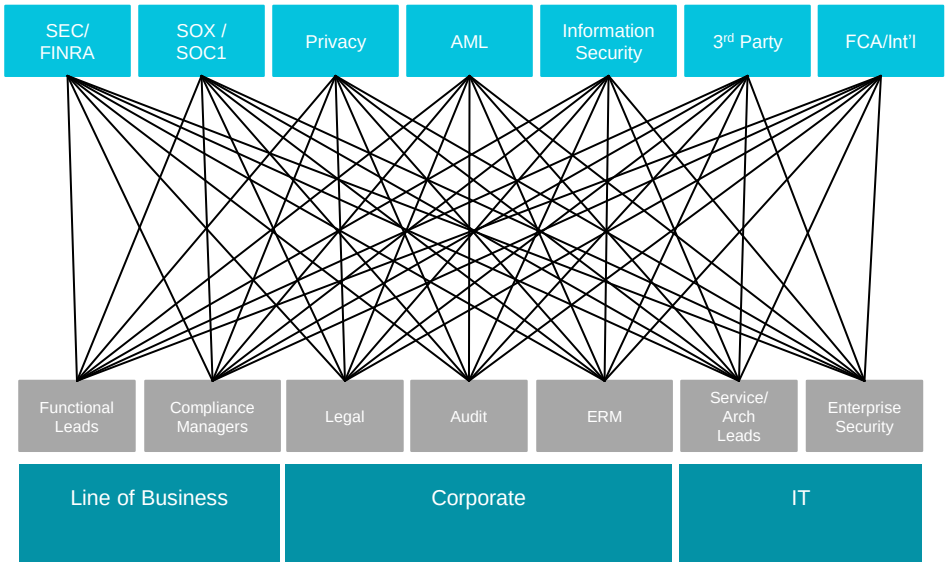
- Client expectations regarding risk management practices have deepened
- Increasing regulatory scrutiny (SEC/FINRA/FCA) with growing expectations around risk management
- Auditor testing is becoming more comprehensive due to our expanding business model and external regulatory expectations (PCAOB)

Evolve our Enterprise Risk Management Program to address

We need improvements to achieve integrated risk management

Our enterprise risk & compliance capabilities have grown in recent years but without an integrated approach.

Program Silos



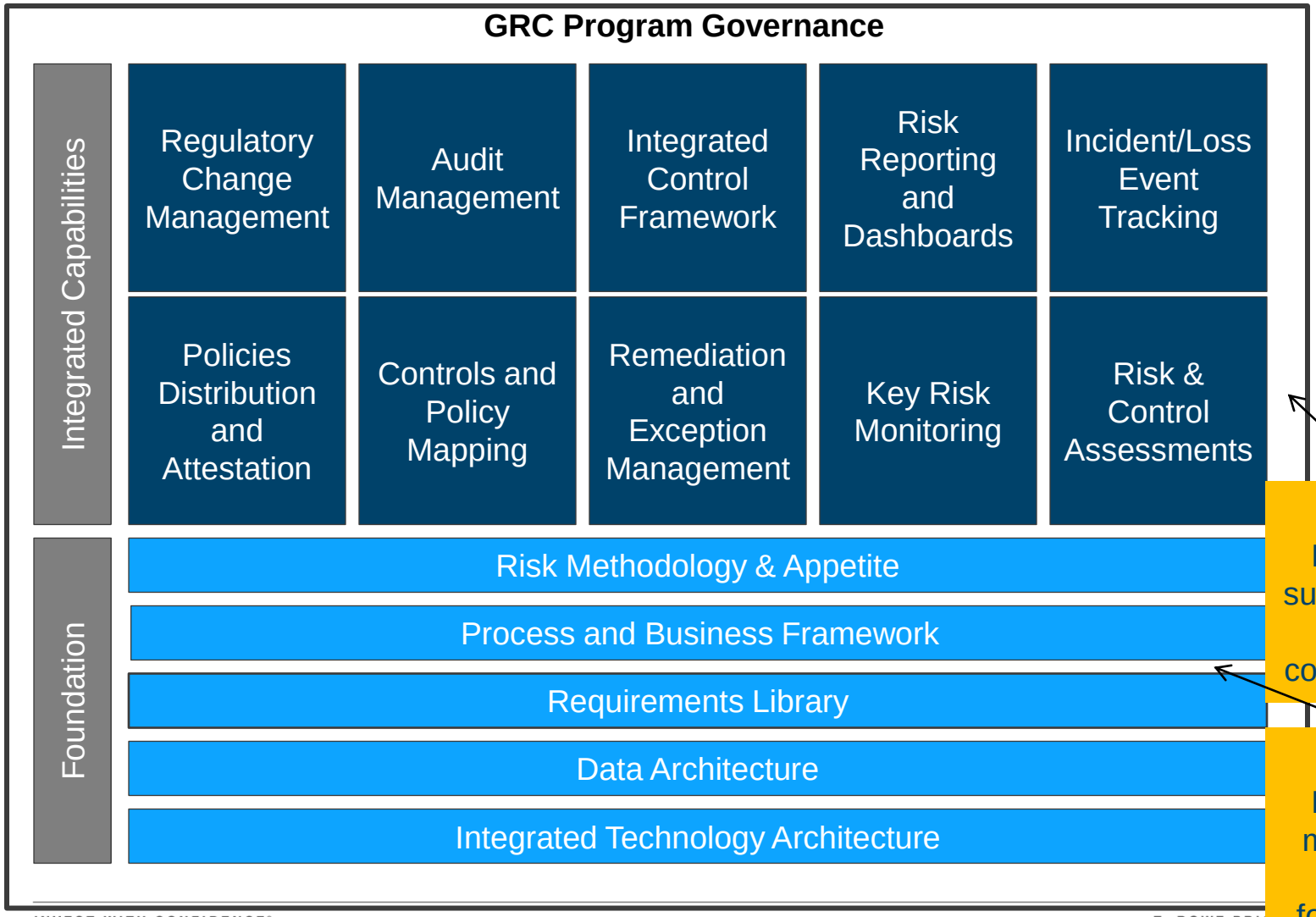
Current Impacts to Quality, Effectiveness & Cost

- Assurance and other organizational functions view requirements, operating environment, risks and controls differently, for example:
  - Internal Audit, Firm-wide Compliance, ERM and IT Risk use different processes and tools that may produce different results
- Higher costs and extra work are needed to support risk and compliance
- Duplication of effort due to a lack of a single source of business risk and control requirements
- Business frustration from being audited and assessed by different functions for essentially the same issues
- Inability to perform trending and analytics due to limited visibility and aggregation
- Business areas are often confused about the roles of Compliance, Risk and Audit

We need a Governance, Risk & Compliance (GRC) strategy with integrated technology to improve risk management

An integrated Enterprise GRC Strategy provides leverage

An integrated risk and compliance management framework provides the ability to assess once, test once, and satisfy many risk and compliance requirements– enabling the business to better identify risk, reduce cost, save time and optimize reporting while providing assurance to management that top risks are addressed.



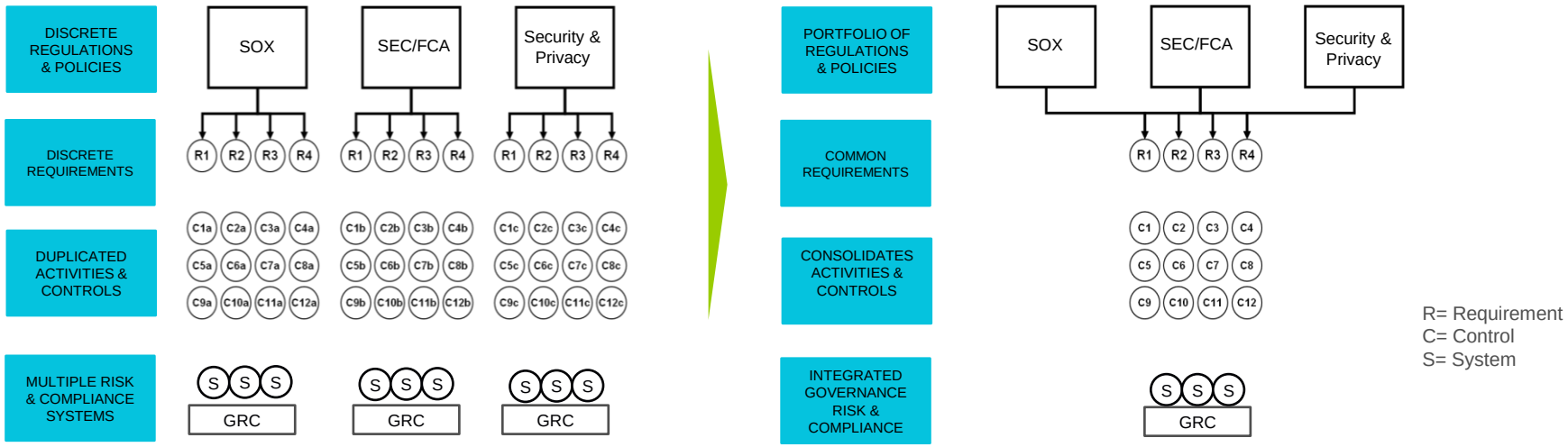
More efficient approach allows for more effective risk management

Overlap

Current “one-off” approach creates multiple discrete programs which leads to inconsistency and inefficiency in managing multiple requirements

Harmonized

Integration that reduces the cost, complexity, and workload is needed; cost efficiencies can be realized when the overlap is removed and a common definition of requirements is applied



R= Requirement
C= Control
S= System

- A core GRC solution provides a comprehensive and standardized view of key risk indicators and enterprise reporting. Types of views that a GRC solution provides include:
  - Business unit/Line of business
  - Corporate reporting against risks associated to a BU
  - Holistic view of enterprise risk (top down and bottom up)
- The GRC solution enables accountability of processes and controls with an enterprise view of risks, risk decisions, controls and associated reporting.

Enterprise GRC is a transformative approach to managing risks confronting the firm

Governance, Risk and Compliance (GRC) benefits

Corporate benefits	Assurance function benefits	Line of business benefits
• Comprehensive risk oversight and management • Improved alignment with external expectations • Enhanced transparency and consistent definition of risk throughout the organization • Improved visibility of risks • Better strategic planning based on risk insights • Integrated and more cost effective maintenance of technology	• Comprehensive risk oversight and management • Aligned risk, control and compliance processes • Integrated view through a common reporting platform that can enable linkage to various "boutique" solutions (i.e. policy, fraud and contract management) • Enhanced risk mitigation techniques through assigned accountability, tracking and reporting	• Tools and evidence for better decision making based on effective risk reporting • Improved risk and compliance integration and management cross-geography and across LOBs • Ability to broadly understand and manage risks facing T. Rowe Price beyond individual LOB's limited view • Ability to contribute and or leverage the common risk repository to enhance coordination for risk mitigation • Reduced audit & assurance fatigue

Next Steps at T. Rowe

- Dialog has started with senior management on evolving ERM:
  - ERM has increased business areas' risk awareness and knowledge over the past few years; now we need to deepen and embed with a common, holistic approach
  - GRC Strategy is a foundational need to achieve this
- Consultant engagement underway to assess current state and develop the roadmap to implement GRC strategy

Lessons Learned

Point	Things to Consider	
We needed to start somewhere with eGRC	The “first one in” could make some critical decisions, but no one wants a huge burden getting started	• Be deliberate in what components you start with • Determine the long-term eGRC strategy early as current decisions can have a long-term impact • In the early stages, determine and apply gold sources for information to prevent variances
eGRC can support different business objectives	The platform worked well in supporting “siloed” components until ERM came along	See above
It’s people and leadership first	People are motivated to achieve their business goals/objectives: • Everyone (business & IT) needs to understand the GRC philosophy and the value to the enterprise; otherwise they pursue their objectives • Engage leadership so they understand the value of GRC and can incent (or mandate) a GRC strategy; it is unlikely to happen organically	• Don’t assume everyone has identical knowledge and/or perspectives; it’s amazing how they vary around the “simple stuff” (e.g. what business activities support which subsidiaries)
Governance is essential	• Governance has to start on the business side- the GRC strategy- as well as with the technology	
End user experience matters	• Don’t underestimate this, particularly now with the higher consumerization of technology	• Adoption is easier if the processes and screens are intuitive