



Continuous Controls Monitoring

Virginia ISACA January Meeting

19 January 2010

Today's Agenda

- ▶ What We Are Hearing About...
 - ▶ Risk
 - ▶ Internal Controls
 - ▶ Continuous Control Monitoring
- ▶ What is CCM?
 - ▶ Framework
 - ▶ EY Point of View
 - ▶ Stakeholder Involvement
 - ▶ CCM Approach
- ▶ Appendices
 - ▶ Success Stories
 - ▶ Lessons Learned

“Making compliance repeatable, sustainable, and cost-effective must become the priority for ongoing investment. Continuous monitoring and automated testing is maturing in approach and applicability to be considered for evaluation now rather than later.”

John Haggerty, AMR
Research Alert

What We Are Hearing About Risk

Keep Us Out of Trouble

Growing Number of Restatements

Bigger Fines and Settlements

Expanding Regulation

Stiffer Sanctions

Catastrophic Reputational Consequences

Criminal Indictments

Make Our Business Better

Coordinated Risk Activities

Enhanced Business Processes

Optimized Controls

Effective Use of Technology

Improved Risk Reporting and Disclosure

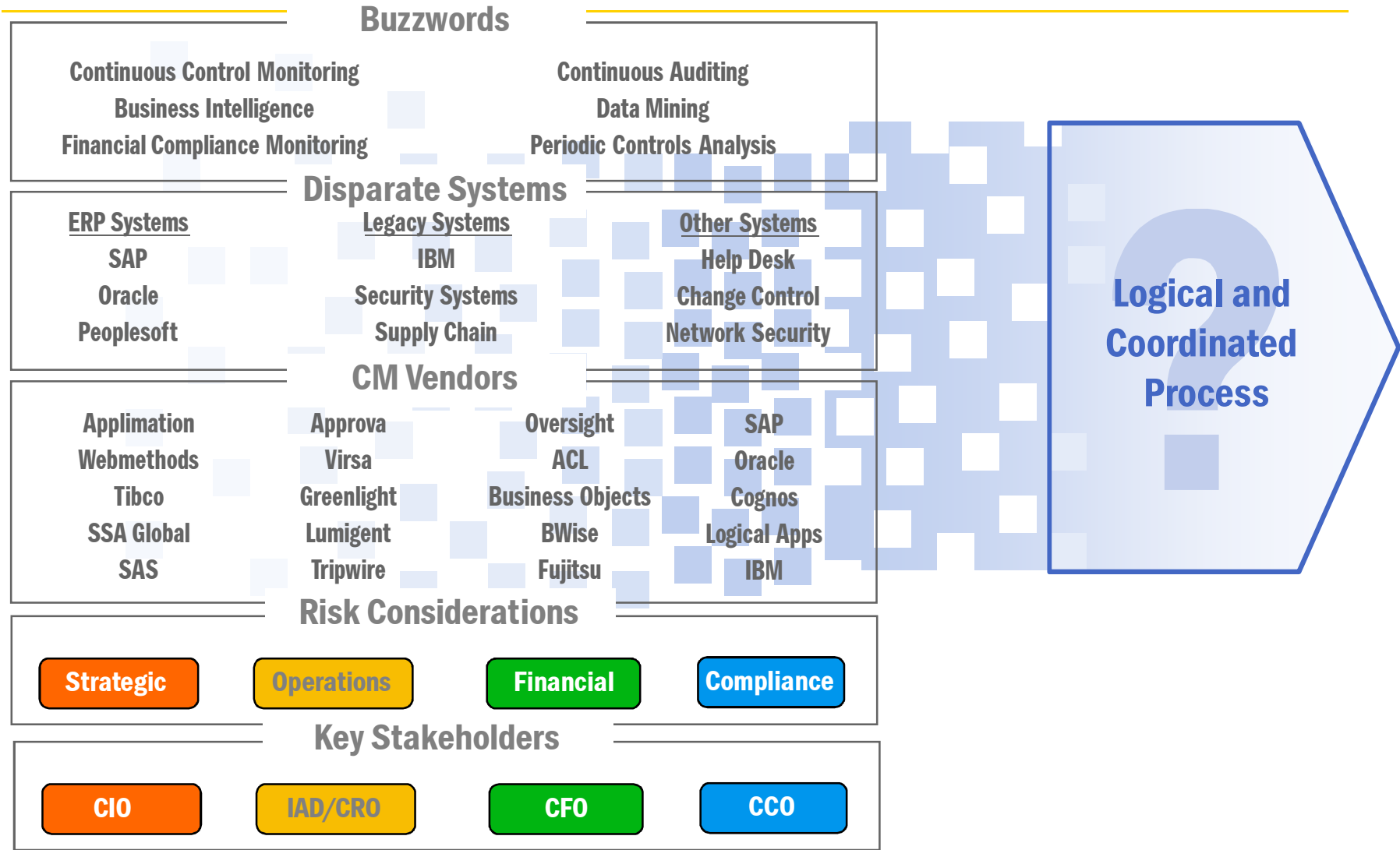
Reduced Total Risk Spend

goal

All too confusing and overdone...
Except when we get in trouble

Must do it...
But how do we do it better?

Why Can CCM Be So Confusing?



What We Are Hearing About CCM

Issues

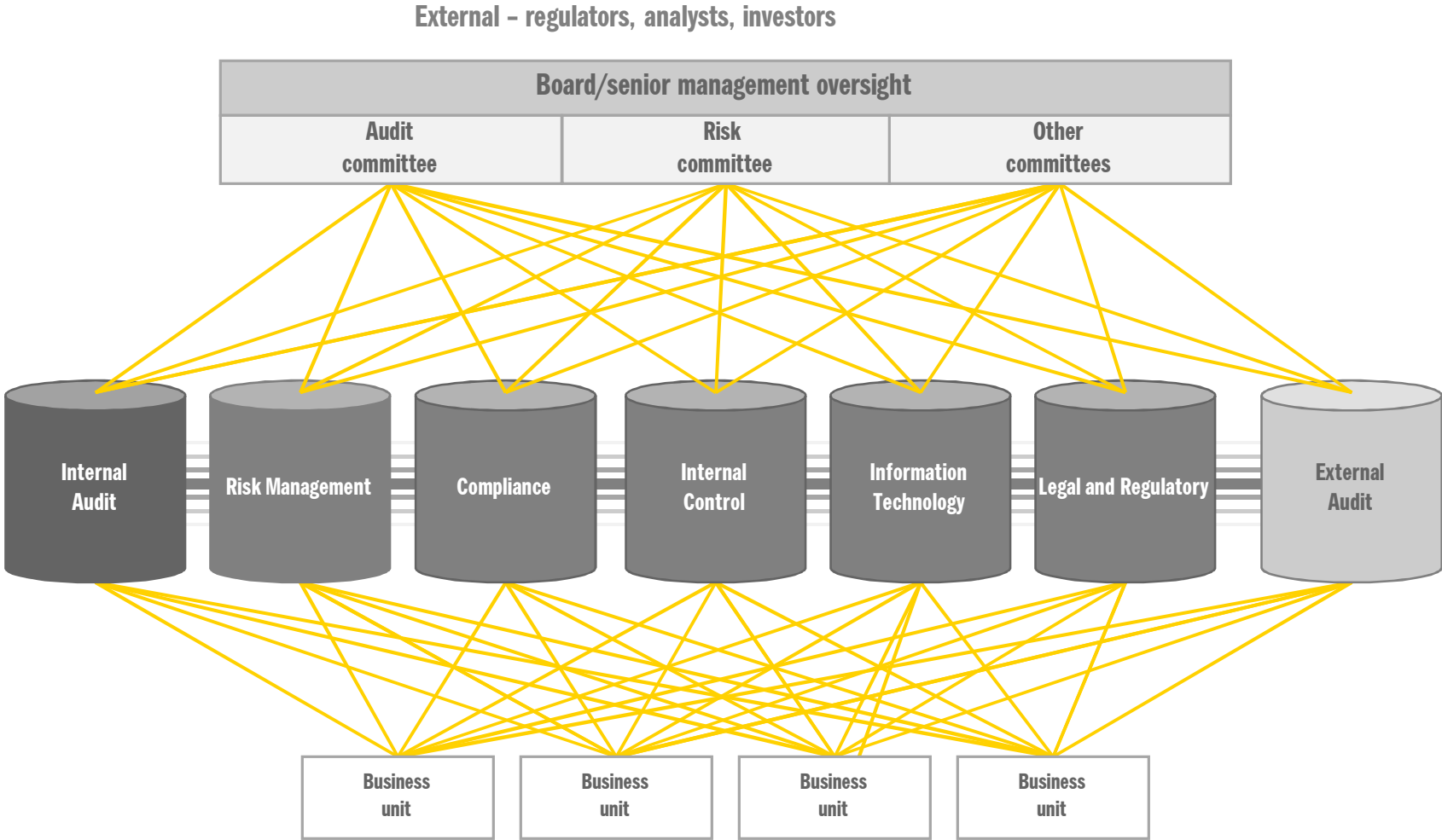
- ▶ **COST OF COMPLIANCE**
 - ▶ Most organizations have spent significant time and money becoming SOX compliant and are concerned about the high cost of compliance
- ▶ **MANUAL CONTROLS**
 - ▶ Many of the controls that organizations have put in place are manual and labor intensive
- ▶ **QUESTIONABLE ROI**
 - ▶ In most cases, the business benefit of SOX investment is not readily visible and the cost of maintaining the manual controls environment is not sustainable
- ▶ **OVERALL AUDIT SCOPE & COSTS**
 - ▶ Managing audit scope and costs are an increasing concern, both from internal and external audit perspectives

Implications

- ▶ **NEED TO BE MORE EFFICIENT**
 - ▶ Most organizations believe they need to do something to be more efficient in automating and monitoring controls
- ▶ **NEED TO BE MORE COST-EFFECTIVE**
 - ▶ Most organizations cannot sustain the increased compliance costs long-term
- ▶ **SOFTWARE TOOLS & SOLUTIONS**
 - ▶ Software vendors are developing and actively promoting new tools and techniques to automate the monitoring of controls (i.e., Approva, Applimation, Logical Apps, Virsa, etc.)

CM can help organizations enhance risk management efforts, as well as drive value for the business

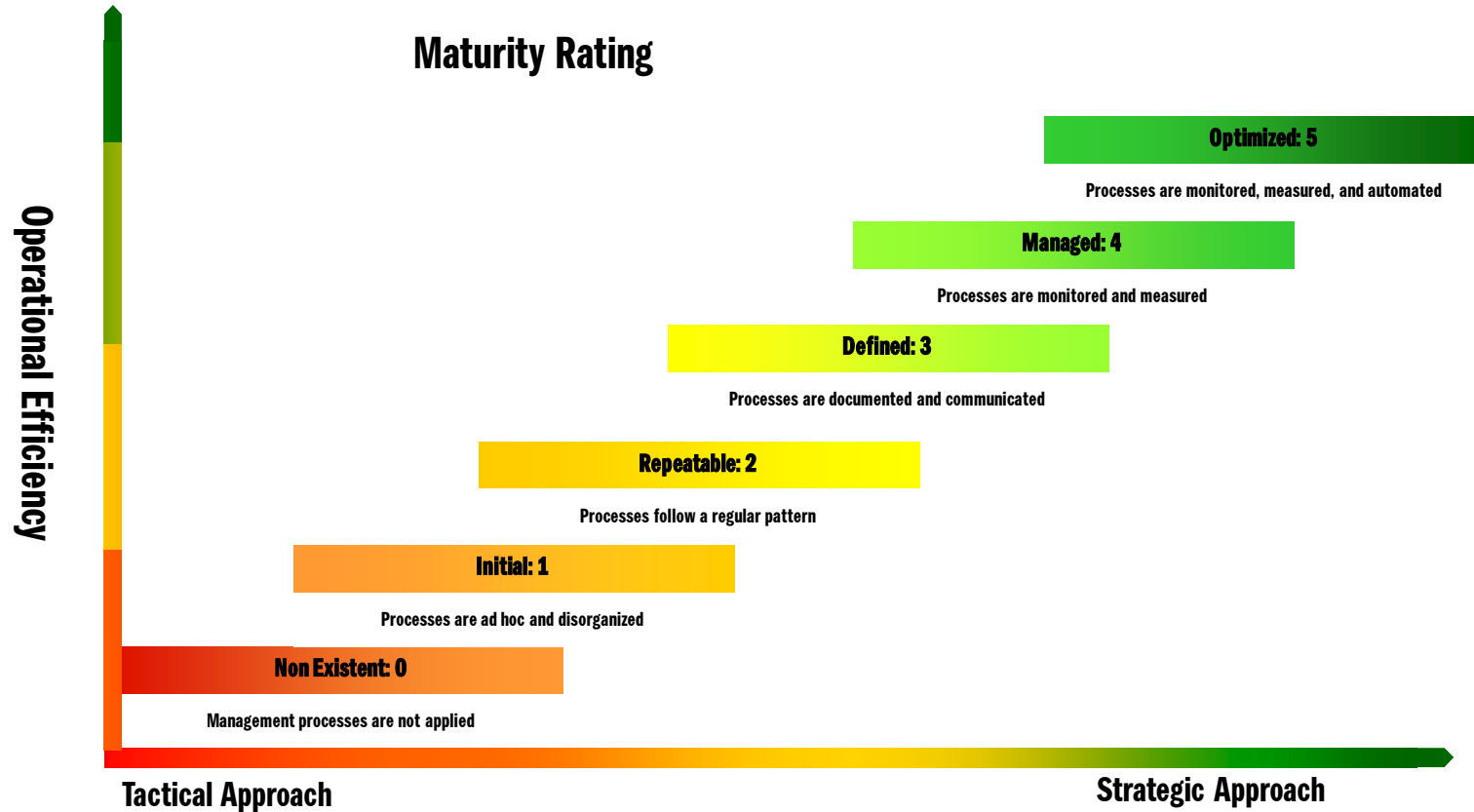
How do risk and control activities impact your organization?



Current State Limitations

- ▶ **Definition of GRC**
 - ▶ The definition of GRC differs from client to client and vendor to vendor, leading to an inability to standardize GRC requirements and guide future development
- ▶ **Isolation of Financial Risk Management Functionality from Mainstream GRC Solutions**
- ▶ **No Single Solution Available**
 - ▶ All solutions perform well for certain aspects of GRC, but no one solution provides a complete holistic solution for all GRC requirements
- ▶ **Immature Dashboarding and Metrics**
 - ▶ Not all tools provide web enabled reporting and dashboards
 - ▶ Non Financial RM tools do not provide advanced charting capabilities to address complex risk scenario analysis
- ▶ **Real Time Data Feed Integration**
 - ▶ Not all tools have robust data integration services that allow for real time data correlation with other risk and monitoring tools.
- ▶ **Virtually Non-Existent Global Regulatory Content**
- ▶ **Inconsistent Framework Mapping and Content**
- ▶ **Configuration Flexibility**
 - ▶ Only a select few tools provide a minimal amount of configuration flexibility, which allows clients to mold the tool to their business processes and taxonomy
- ▶ **Assessment Methodology**
 - ▶ Only a select few tools allow for logic based assessments (questionnaires, survey's, etc.), which integrate business workflow and risk calculations driven by assessment results.
 - ▶ Risk Control Library management is not integrated into assessments to drive risk convergence.

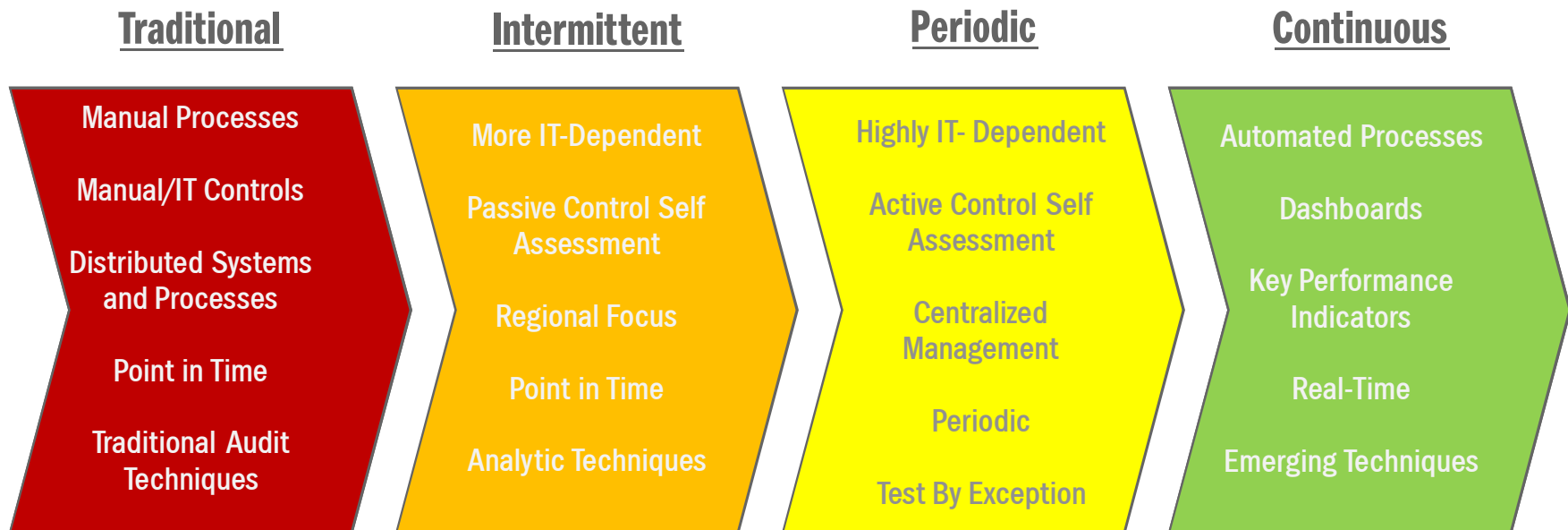
GRC Maturity Progression



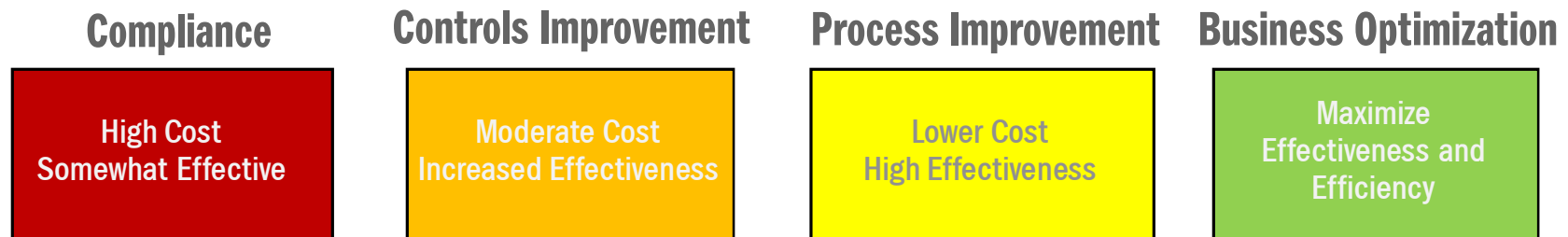
IT-GRC Approach & Maturity

The Evolution Of Internal Controls

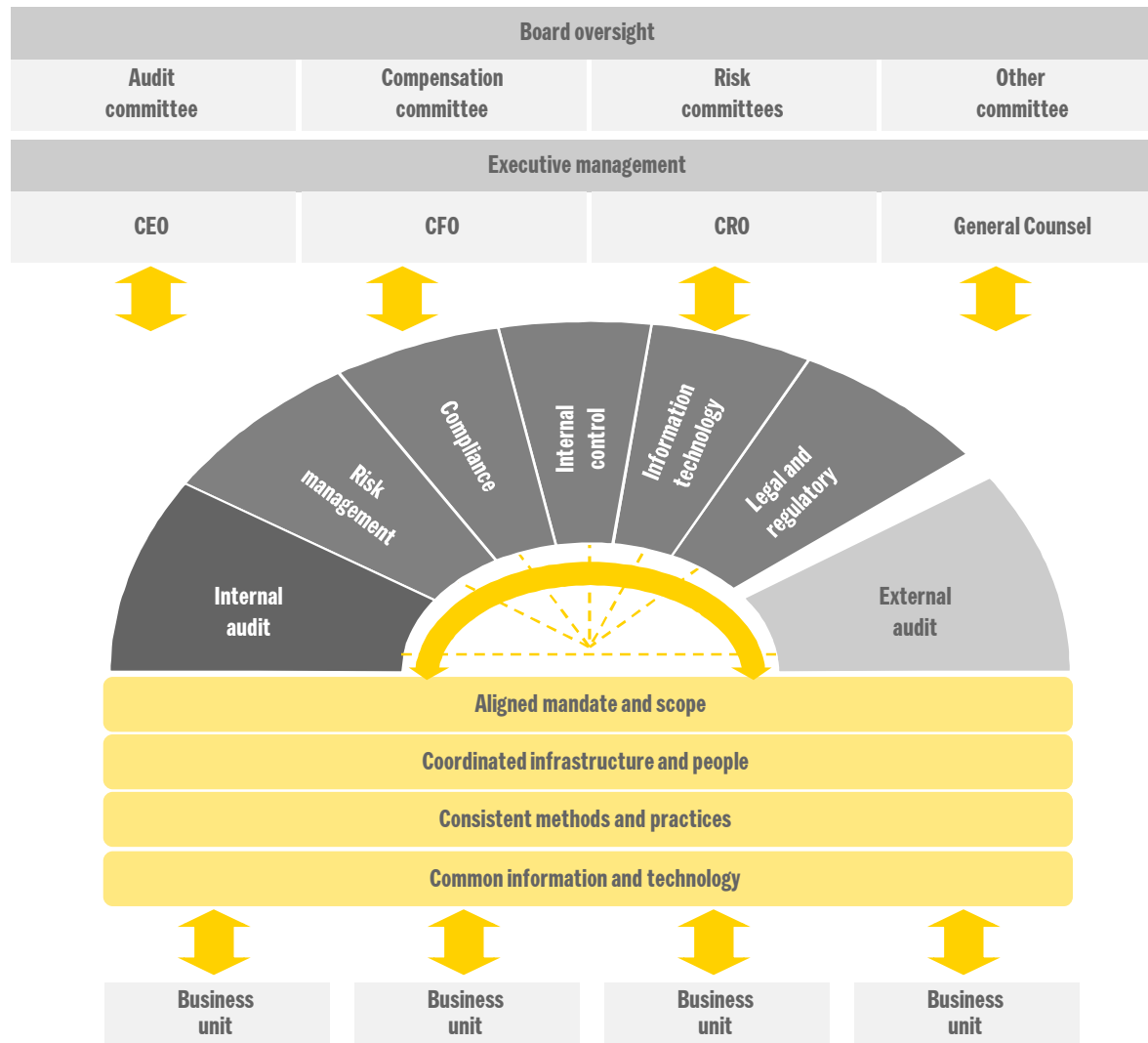
Control Maturity Levels



Objectives/Focus Areas



What is the future of risk for your organization?



Clearly Defined Responsibilities

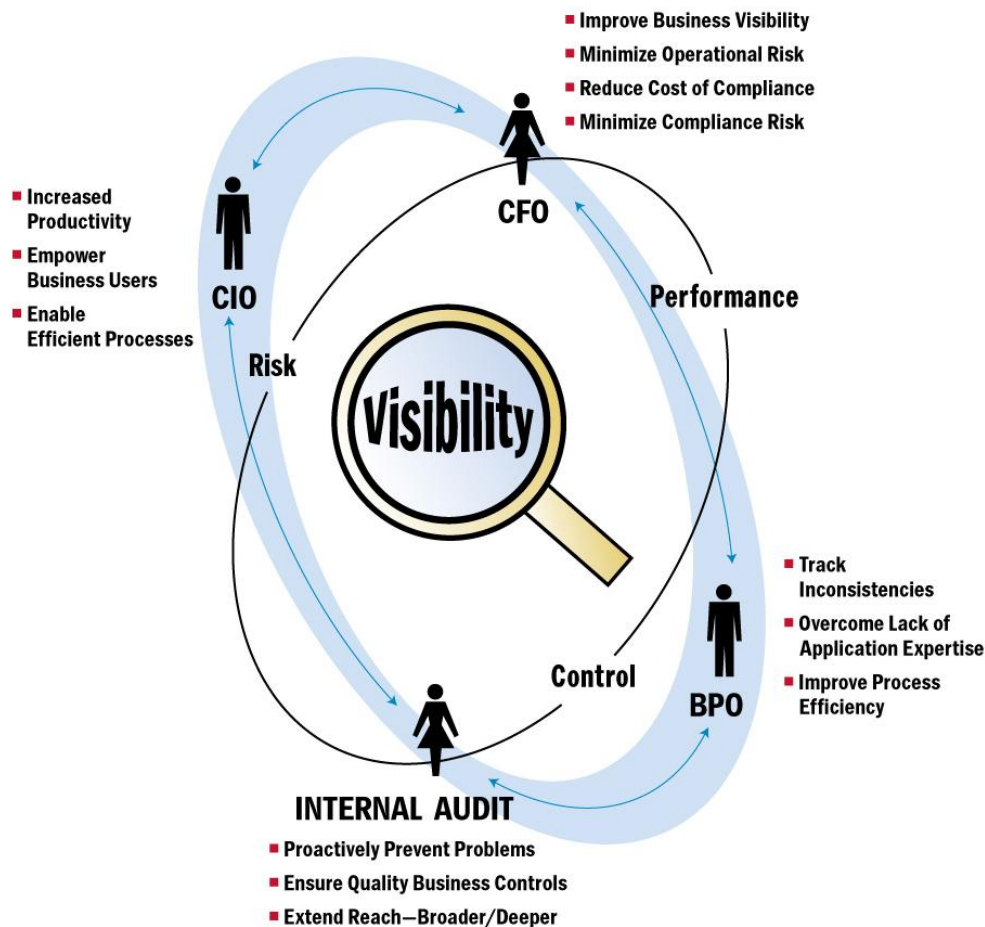
Clear and comprehensive risk reporting

Opportunity to Leverage/ Coordinate with other control functions

Foundations of Convergence

Efficiency and Effectiveness

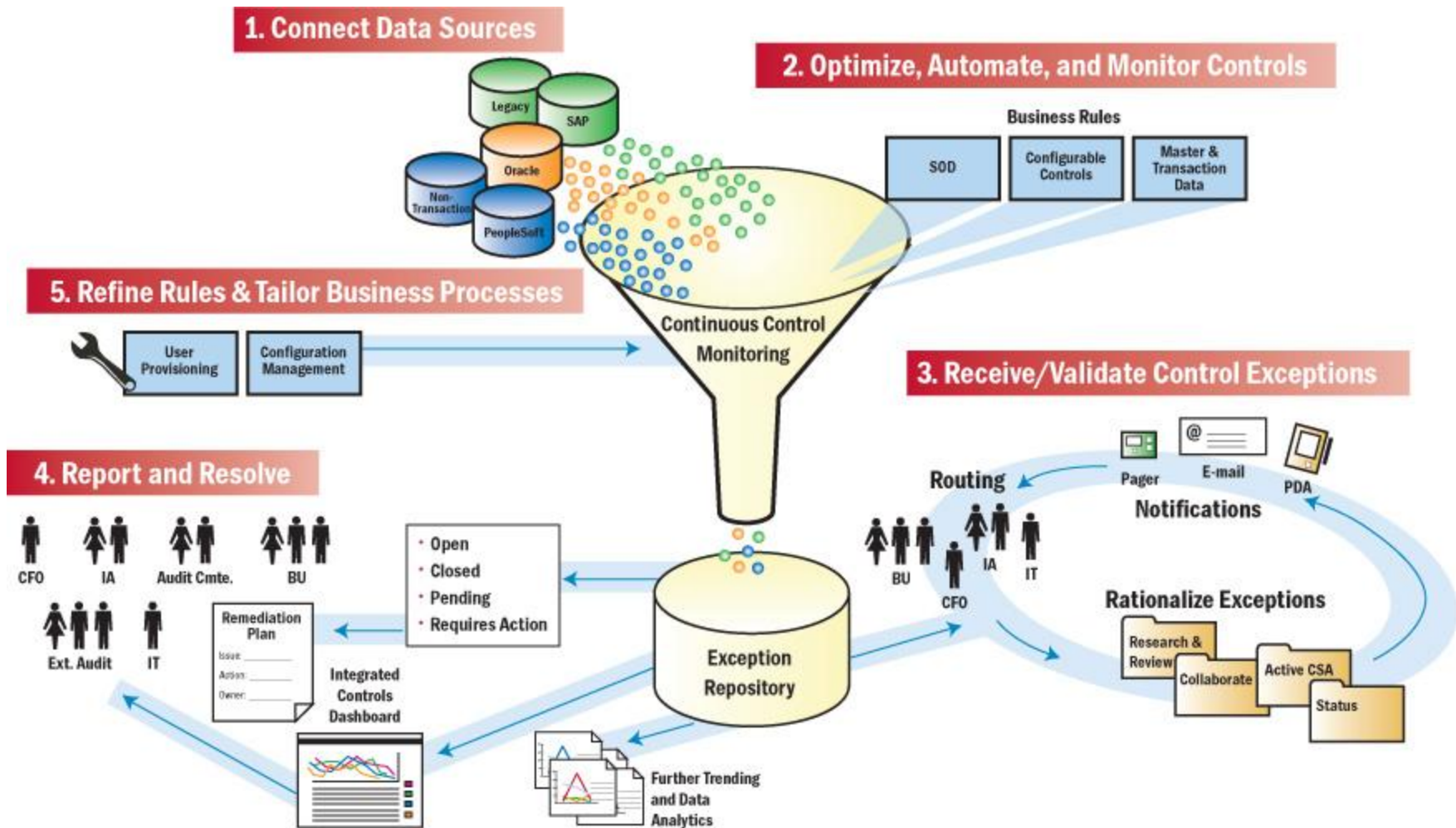
Approaching CCM: *Stakeholder Involvement*



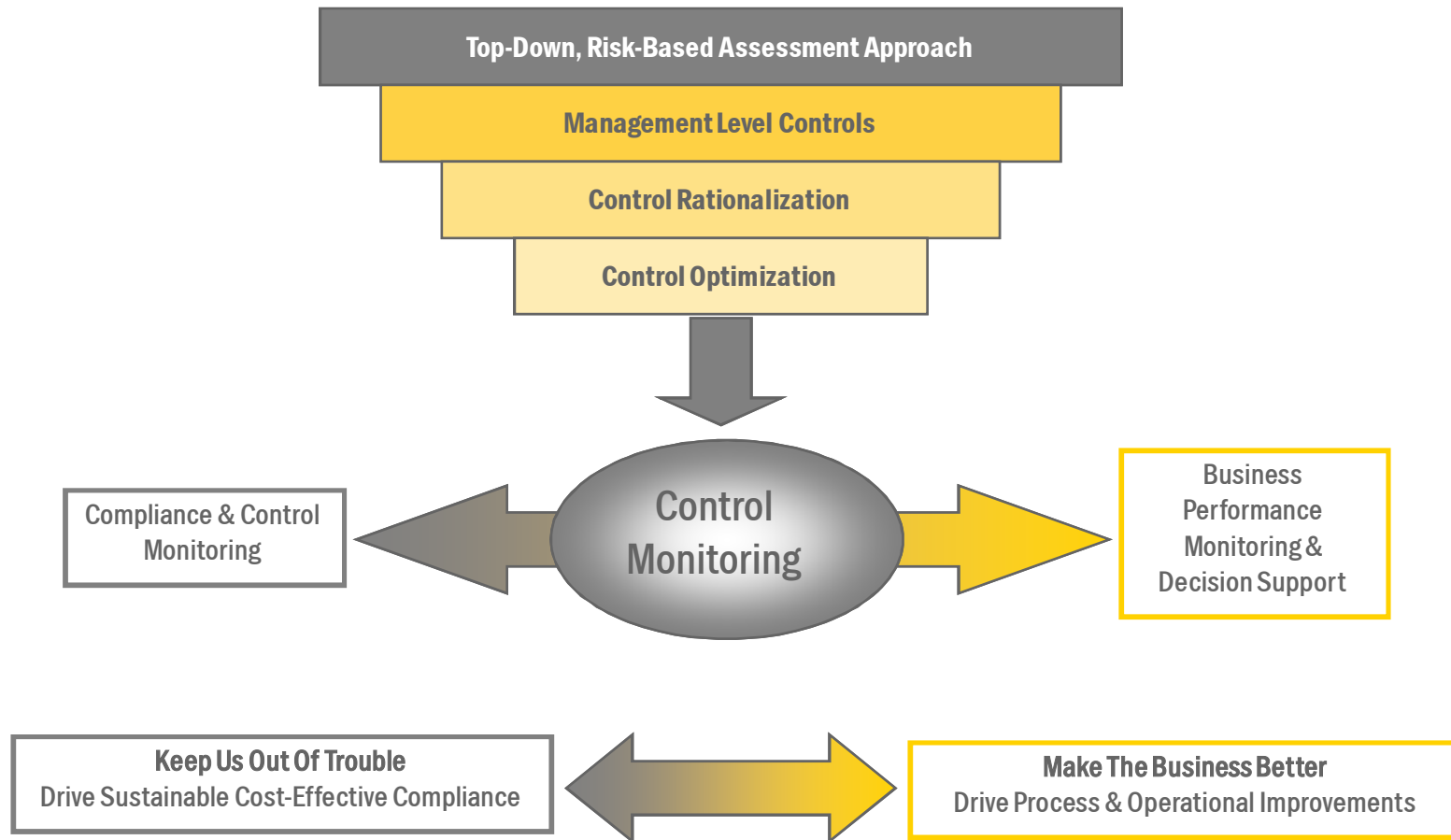
Considerations

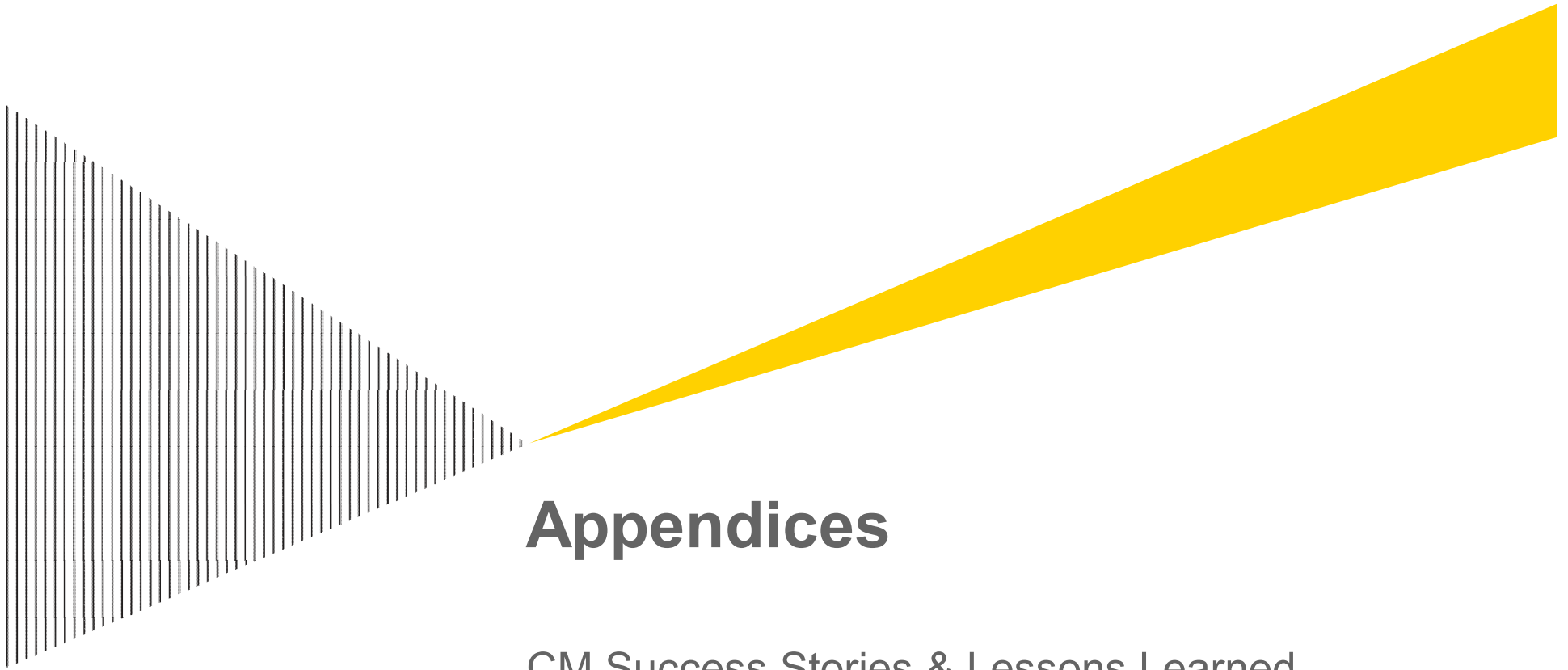
- ▶ *Sponsorship*: Active executive sponsorship and commitment to change the control environment
- ▶ *Collaboration*: Require participation from a broad range of functional areas (i.e., Procurement, Finance, IT, SOX Leaders, Internal Audit, Divisional Executives, etc.)
- ▶ *Scope*: Begin with the end-state vision, but implement a narrow initial scope and build on success
- ▶ *Approach*: Apply as a “horizontal” solution that applies to performance, risk, and controls across the entire business
- ▶ *Communication*: Provide ongoing internal and external communication
- ▶ *Prioritization*: Identify and redesign processes and controls that currently cause the most “pain” or present the most risk (i.e., overall prioritization of efforts) or will deliver initial value to support the continuing business case

Approaching Continuous Controls Monitoring



Ernst & Young's Point Of View On CCM

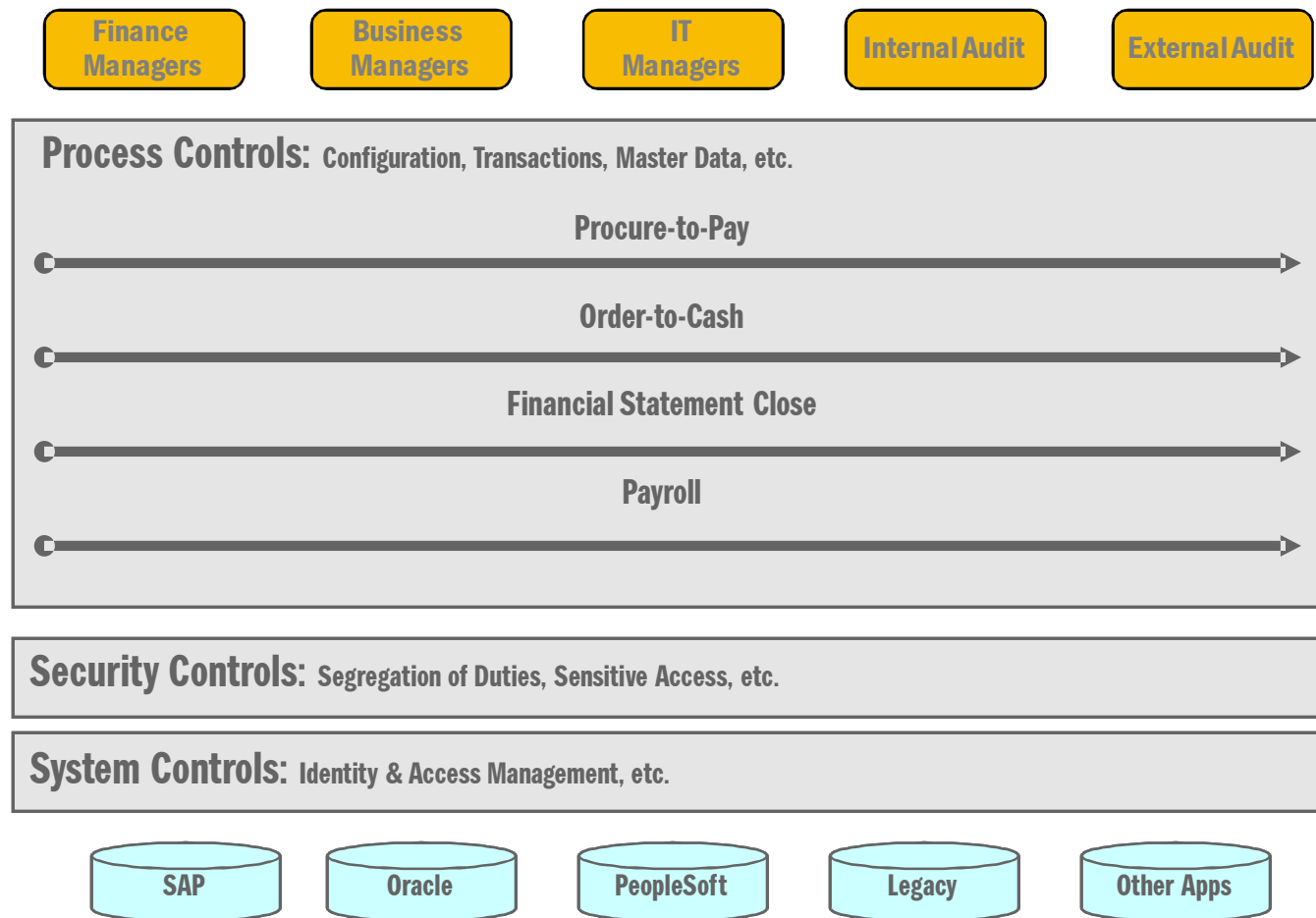




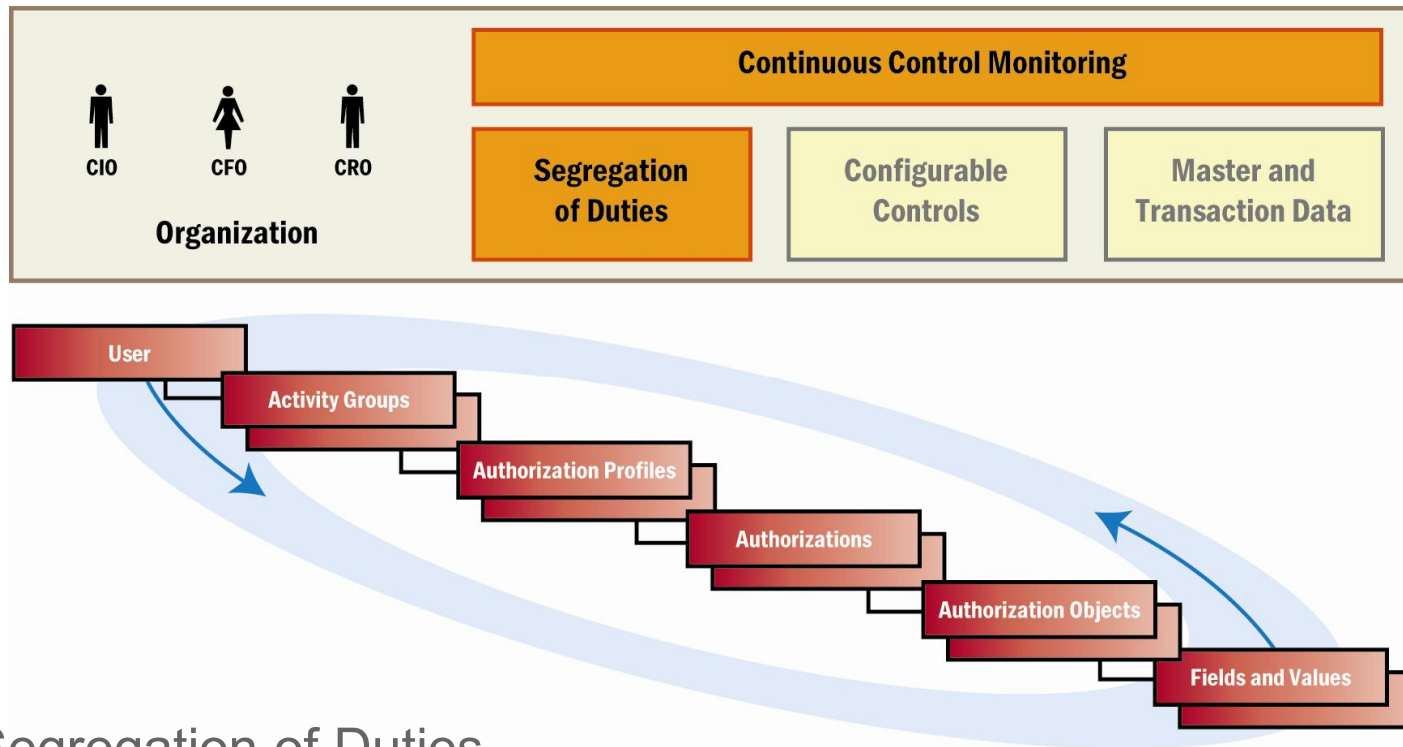
Appendices

CM Success Stories & Lessons Learned

Continuous Controls Monitoring Scoping

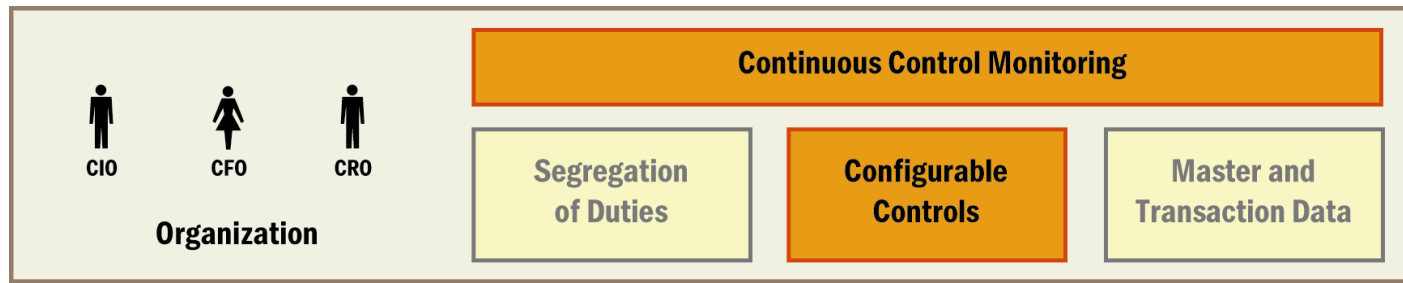


Begin with Proper Segregation of Duties



- ▶ Segregation of Duties
 - ▶ Detect and/or prevent user access and segregation of duties violations
 - ▶ Identify and monitor users with access to sensitive transactions
 - ▶ Facilitate the user provisioning and periodic access review process

Leverage Controls in your Applications

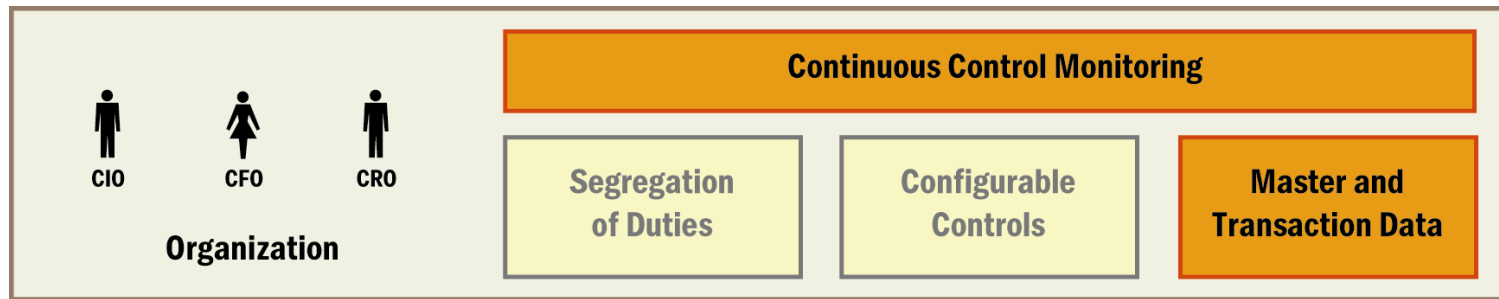


This screenshot shows the SAP Receiving Options (E2) configuration window. The "Miscellaneous" section is circled in green, highlighting the "Allow Substitute Receipts", "Allow Unordered Receipts", "Allow Express Transactions", "Allow Cascade Transactions", and "Allow Blind Receiving" checkboxes. The "Over Receipt Control" section shows a tolerance of 10% with a "Warning" action. The "Receipt Routing" is set to "Standard Receipt" with a "Warning" action. The "Receipt Number Options" section shows an "Automatic" action and a "Numeric" type.

This screenshot shows the SAP Receiving Options (C2) configuration window. The "Miscellaneous" section is circled in green, highlighting the "Allow Substitute Receipts", "Allow Unordered Receipts", "Allow Express Transactions", "Allow Cascade Transactions", and "Allow Blind Receiving" checkboxes. The "Over Receipt Control" section shows a tolerance of 5% with a "None" action. The "Receipt Routing" is set to "None" with a "None" action. The "Receipt Number Options" section shows an "Automatic" action and a "Numeric" type.

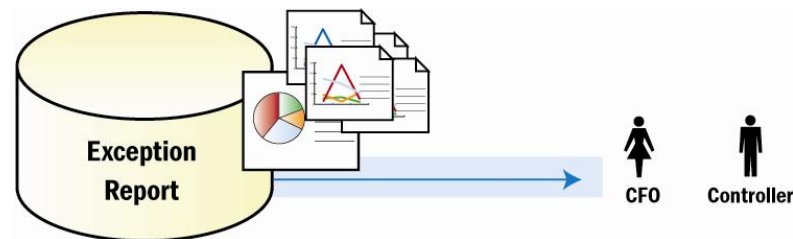
- ▶ Configurable Controls
 - ▶ Alert appropriate personnel when critical configuration controls and master file changes have occurred
 - ▶ Verify system patches and routine changes do not impact the integrity of the configurable controls
 - ▶ Enable companies to compare configurable controls across business units

Implement proper Data-level Controls



▶ Master and Transaction Data

- ▶ Identifies exceptions and enables the organization to react quickly
- ▶ Reflects audit's substantive testing approach for key controls and use of data analysis technologies
- ▶ Allows quantification of control deficiencies and aids in the identification of potential Fraud
- ▶ Monitoring of KPIs enables intelligent business decisions and identification of areas for improvement



Ernst & Young Observations / IT-GRC

- ▶ All of the IT-GRC specific tools come from vendors who have in the past served niche markets, or are new players in the IT-GRC market space. This niche vendor approach lead to extreme specialization in the tools. This lead to certain tools being strong in certain IT-GRC disciplines, and weak in others.
- ▶ As the need for a robust, mature, and complete GRC solution has been identified, these vendors have begun to evolve or develop their tools to meet the demands of the market, but are several years away from providing a complete IT-GRC (or E-GRC) tool.
- ▶ Currently there is no tool that can provide an out of the box complete holistic IT-GRC solution. There is a tool that can provide a complete solution, but it requires a tremendous customization effort, which would have to be supported by the client.
- ▶ There are several tools that can provide functionality across the majority of an IT-GRC program, but the best approach would be a combination of tools (until the vendor solutions mature or consolidate, when perhaps a single vendor solution may emerge).
- ▶ Existing solutions at client locations may be leveraged for certain aspects of an IT-GRC program, but no one tool can be used for the entire IT-GRC program (unless the client is willing to support extensive customization for a single tool). The best approach for situations like this would be to determine your requirements for an IT-GRC program first, then determine your current solution that can meet any of the requirements.

CCM Success Story 1: Manufacturing

- ▶ Profile
 - ▶ Fortune 1000 Manufacturing Company
 - ▶ Global & Decentralized Operations
 - ▶ Implementing a single global Oracle ERP instance
- ▶ Business Drivers
 - ▶ Reduce the cost of compliance and the impact it has on the corporate culture
 - ▶ Business process automation and improvement to gain competitive advantage
- ▶ CCM Vision
 - ▶ Oracle centric CCM solution
 - ▶ Ability to assess, automate and monitor controls related to user security/segregation of duties, configurable setups and transactions/master data
 - ▶ Enhance certain processes such as user provisioning and configuration management
- ▶ Result
 - ▶ The ROI was much better than originally planned (greatly reduced cost of compliance)
 - ▶ Our efforts were initially driven solely by compliance but quickly shifted to identifying areas of process improvement and optimization

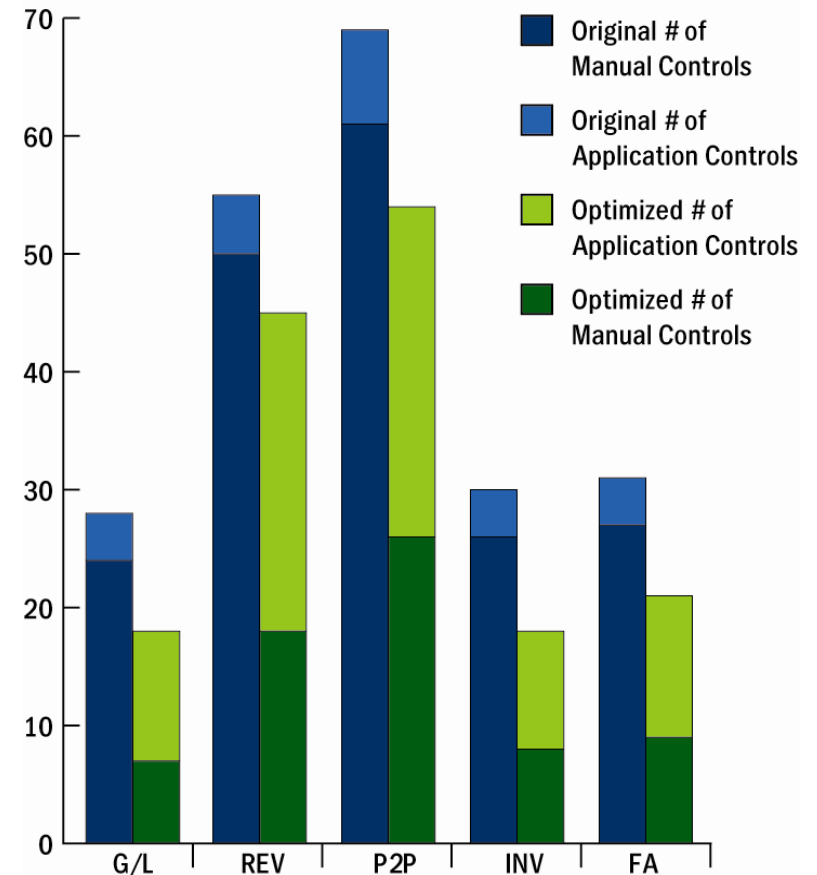
CCM Success Story 1

Key Accomplishments

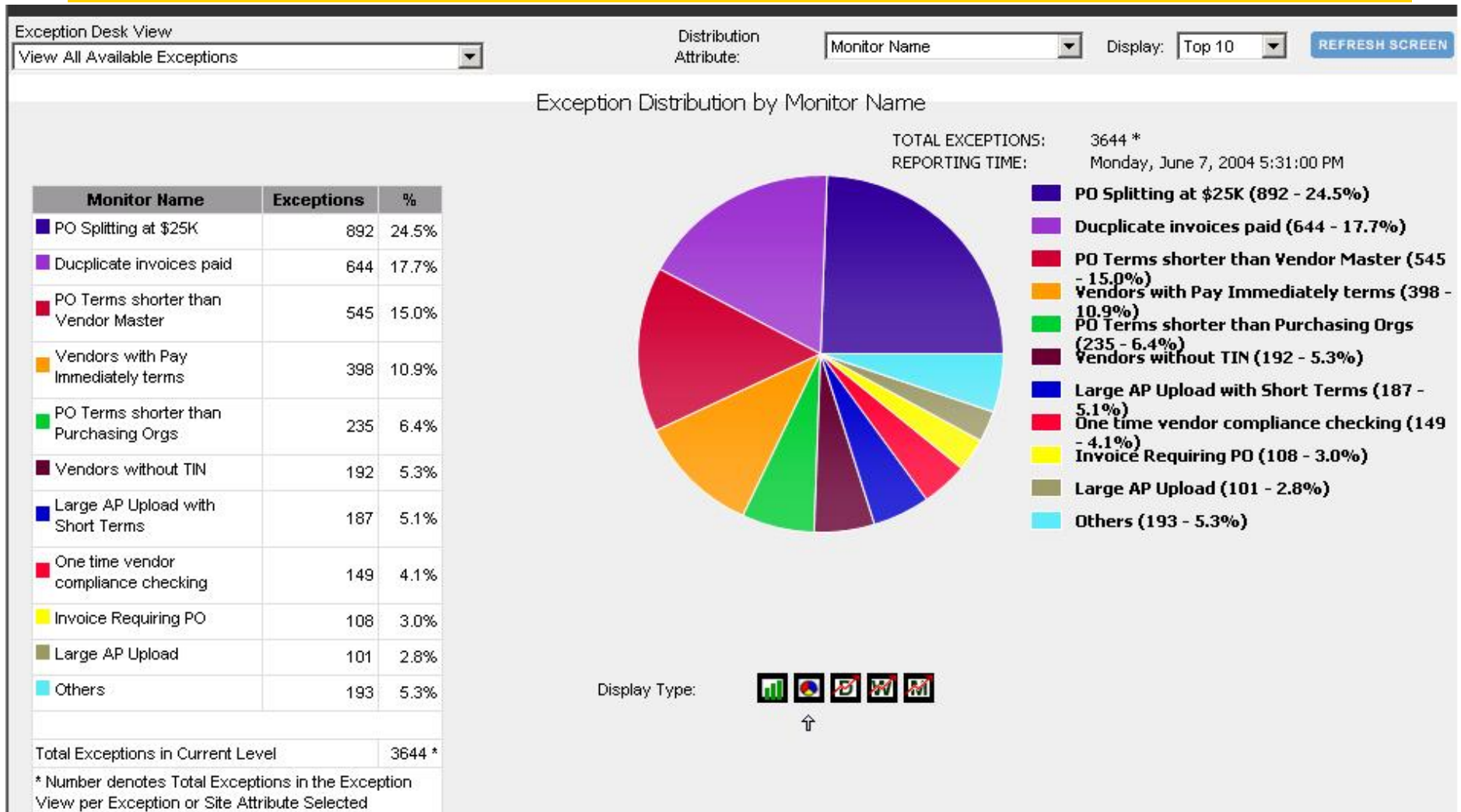
- ✓ Reduced total number of key controls by 21%
- ✓ 56% of remaining key controls are application-level or automated controls
- ✓ Developed “gold standard” application-level control design
- ✓ External Auditor relied heavily on this work
- ✓ Continuous monitoring significantly reduced the time required for testing
- ✓ Leveraged the CCM solution to reengineer certain logical access/user provisioning processes
- ✓ Identified, assessed, remediated and monitored operational controls

Controls being Continuously Monitored	
Configurable Controls—SOX	30
Configurable Controls—Operational	71
Segregation of Duties and Access Controls—SOX	50
Total # of Controls being Monitored	151

Summary of Key Controls (by Process)



CCM Dashboard: Monitoring Management Metrics



Lessons Learned

▶ **Business Case**

- ▶ Clearly define the business benefits you are seeking to achieve with Automated Control Testing
- ▶ Compliance: Keep us out of trouble
- ▶ Efficiency: Make our Business Better

▶ **Implementation Scope**

- ▶ Begin with a vision of the end state
- ▶ Realize early value by beginning with narrow initial scope, then build upon early success

▶ **Functional Design Considerations**

- ▶ Determine “ownership” of controls Analysis Rules – design, maintenance, access
- ▶ Determine how best to structure Analysis Rules based on your business objectives
- ▶ Determine degree of Analysis Rule standardization across the enterprise
- ▶ Determine how to manage Analysis Rules across multiple PCA instances (if applicable)

▶ **Data Acquisition**

- ▶ Determine sensitivity of controls data across the enterprise
- ▶ Identify systems to be queried for controls data
- ▶ Determine how to populate non-automated data into dashboard

▶ **Model Controls**

- ▶ Start with internal audit plan and external audit findings; “hot buttons”
- ▶ Begin with a pilot to build momentum with current deficiencies
- ▶ A/P, Payroll, T&E are typically “low-hanging” fruit with the greatest ROI
- ▶ ROI may not be proportional with Non-Routine or Estimated Processes

▶ **Validate Control Exceptions**

- ▶ Involve BU, internal and external auditor early in the process
- ▶ Create a transition path from IA to BU
- ▶ Adjust “thresholds” to limit exceptions being routed to stakeholders
- ▶ Maintain consistent process for exception responses with action forms

▶ **Report and Refine**

- ▶ Provide “root cause” reporting and identify areas for remediation
- ▶ Establish change management process for adding, refining and decommissioning control Analysis Rules
- ▶ Allow BU to take ownership for the control
- ▶ Lend a hand not a stick



Contact Information

Mark E. Whittenberg, CISA | Senior Manager | Advisory Services

Ernst & Young LLP

One James Center, 901 East Cary Street, Richmond, Virginia 23219

Office: +1 804 344 4669 | Mobile: +1 804 205 0550 | eFax: +1 866 399 8613

mark.whittenberg@ey.com

Website: www.ey.com

 **ERNST & YOUNG**

Quality In Everything We Do

Ernst & Young Assurance | Tax | Transactions | Advisory

About Ernst & Young

Ernst & Young is a global leader in assurance, tax, transaction and advisory services. Worldwide, our 130,000 people are united by our shared values and an unwavering commitment to quality. We make a difference by helping our people, our clients and our wider communities achieve potential.

For more information, please visit www.ey.com.

© 2008 EYGM Limited. All Rights Reserved.
Proprietary and confidential. Do not distribute without written permission.

Ernst & Young refers to the global organization of member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients.