Putting Risk & Compliance Decisions Into a Consistent Context

Don Griffith

Massachusetts Mutual Life Insurance Company

Vice President

Putting Risk & Compliance Decisions Into a Consistent Context

A Hybrid Organizational Structure Across Multiple Business Lines/Subsidiaries

- Independent Subsidiaries
- Control function reporting lines vary
  - Some direct, some indirect

The Challenge of Defining GRC

- Need to clarify purpose, goals, expected outcomes
- Historically, control functions acted relatively independently
  - Interaction at senior level, with some coordination at lower levels, but ad hoc
  - Challenge was ad hoc use, with little or no coordination on GRC technology

Putting Risk & Compliance Decisions Into a Consistent Context

Creation of GRC Council

- Consists of General Auditor, Chief Risk Office, General Counsel, Enterprise Information Risk Officer, Chief Compliance Officer
- Chaired by Audit
- Charter
  - Develop, coordinate and implementing the enterprise-wide GRC activities;
  - Review enterprise-wide risk, compliance, information risk, audit, legal and other GRC program-related reports to ensure effective oversight, monitoring and assessment of the enterprise's GRC activities;
  - Establish and oversee the activities of GRC working groups , to which the Council may assign specific GRC activities as it deems appropriate.
  - Provide relevant, reliable and timely information to stakeholders.

Putting Risk & Compliance Decisions Into a Consistent Context

Use of technology as GRC tool in nascent stage

- Need to agree on defined terms (policy, procedure, control, etc.)
  - Quickly discovered we didn't all speak the same language
- Challenge of working in silos is that tools can be just as siloed without coordination
  - Each control function creates tools for its needs, but without coordination, robust insight isn't possible
- Leveraging Risk Taxonomy as basis for uniformity/relational data
- Consolidated issue/mitigation database

Putting Risk & Compliance Decisions Into a Consistent Context

Certain control functions farther along than others

- Enterprise Information Risk/Security
- Audit
- Enterprise Risk Management
- Procurement /Vendor Management
    - Can be particularly challenging to the extent multiple control functions have interest

Integration/coordination remains challenging

Putting Risk & Compliance Decisions Into a Consistent Context

Compliance Integration

- In early stages
  - Risks difficult to quantify
  - Monetary risk often low on a per incident basis
  - Enterprise-wide compliance risks often have great impact, but are relatively low probability
  - How to identify meaningful data to get meaningful results

- Some Early Results
  - Regulatory Repository
    - Issue identification/mitigation integrated into issue/mitigation database
    - Challenge is manual input of data

  - Key Risk Indicators
    - Has potential to better track compliance risks
    - Identification of appropriate KRIs is critical

Putting Risk & Compliance Decisions Into a Consistent Context

Compliance Integration—Some Early Result

- Regulatory Repository
  - Issue identification/mitigation integrated into issue/mitigation database
  - Challenge is manual input of data

- Key Risk Indicators
  - Has potential to better track compliance risks
  - Identification of appropriate KRIs is critical
  - Establishing appropriate thresholds/tolerances
  - Need to define protocols/escalation

Putting Risk and Compliance Decisions Into a Consistent Context

James Rose

Humana

Vice President, Chief Audit Officer

Putting Risk and Compliance Decisions Into a Consistent Context

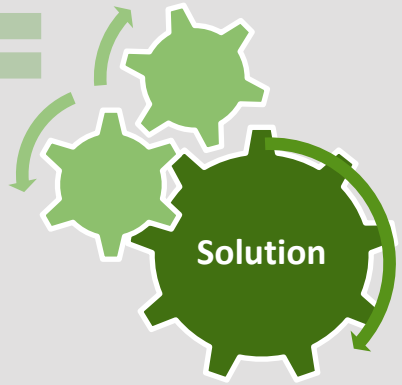
Humana is a leading health care company that offers a wide range of insurance products and health and wellness services that incorporate an integrated approach to lifelong well-being.

- Headquartered in Louisville, Kentucky
- One of the nation's largest publicly traded health and supplemental benefits companies
- Ranked 79th on Fortune's list of largest corporations
- 2012 revenues of approximately $39 billion
- Operates several hundred health centers and worksite clinics nationwide

Putting Risk and Compliance Decisions Into a Consistent Context

Governance, Risk and Compliance Engagement Philosophy

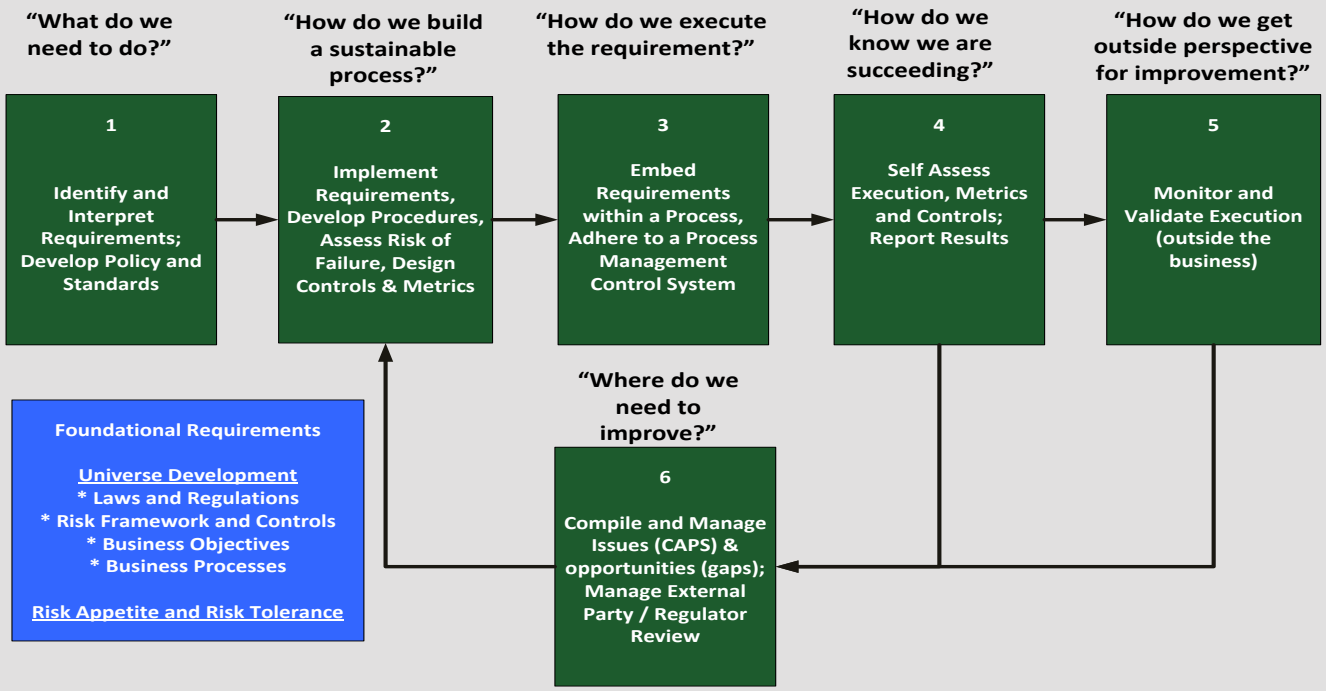
People → Process → Technology =



- **People** = *"Who you are"*
  - Roles
  - Distributed Ownership
  - Access Controls
  - **User Context**
- **Process** = *"What you need to do"*
  - Approach and Workflow
  - Status-driven
  - Content
  - **Business Context**
- **Technology** = *"How you do it"*
  - Learning/Guidance
  - Adaptive
  - Step-by-step
  - **Solution Context**

Putting Risk and Compliance Decisions Into a Consistent Context

We believe that any sustainable, effective & efficient process requires several interrelated steps.



"Our goal is to create great business processes that are efficient, effective, and compliant – as opposed to a compliance process that is separate from the business processes."

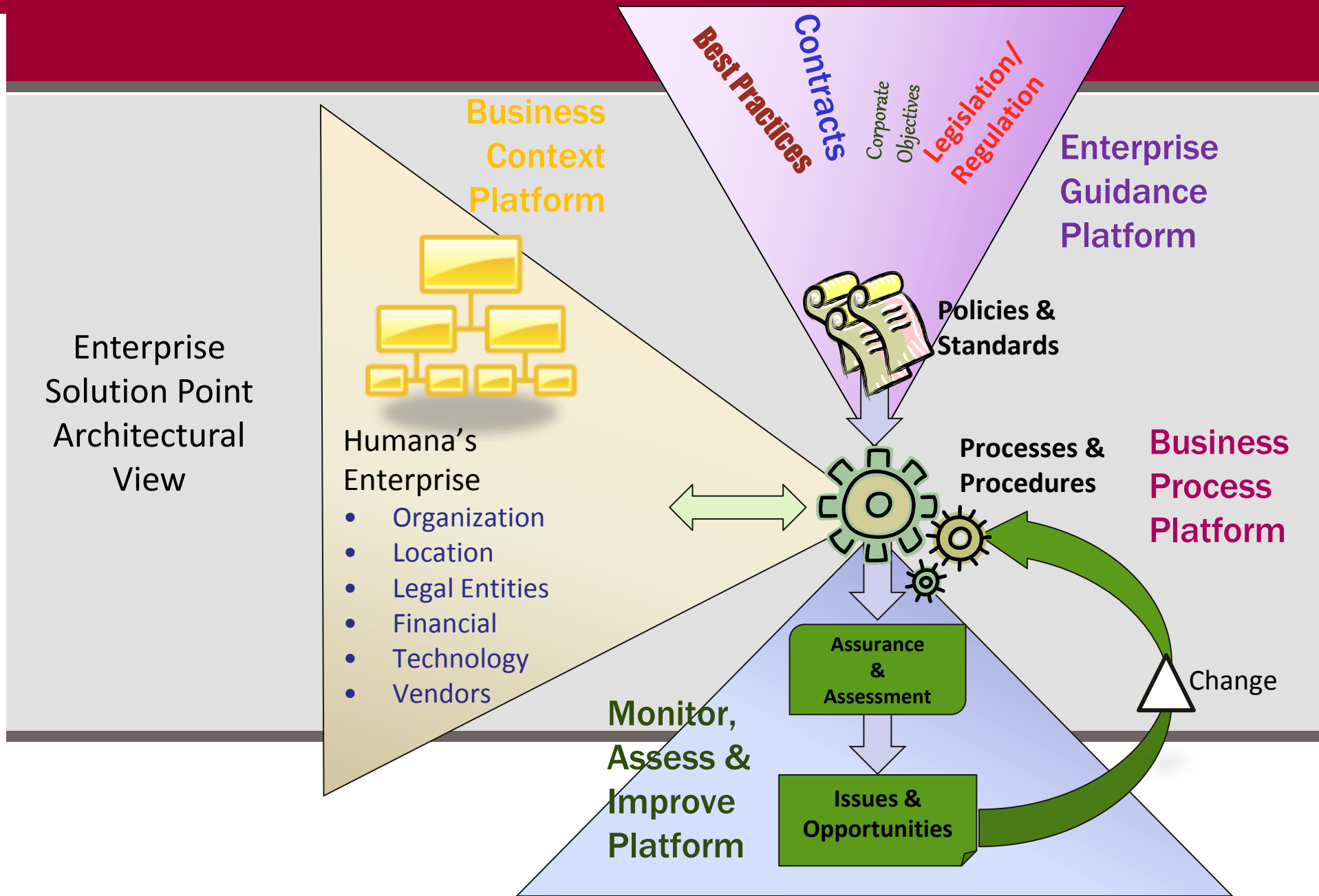
Putting Risk and Compliance Decisions Into a Consistent Context

Enterprise Solution Point – Vision and Objectives

1. Silos to Synergy
2. Clear Guidance
3. Accountability
4. Ask Once, Answer Many
5. Process Automation
6. Transparency

"To make the efforts of our frontline business leaders simpler, more efficient, more transparent, and more effective with regard to managing processes, risk, controls, and compliance"

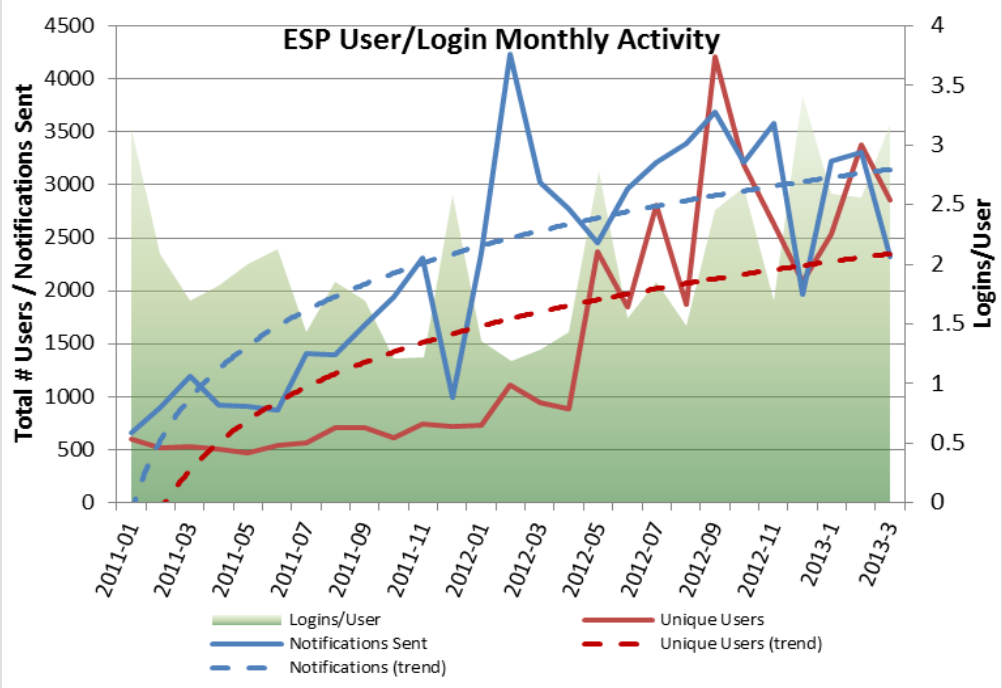
Putting Risk and Compliance Decisions Into a Consistent Context



Putting Risk and Compliance Decisions Into a Consistent Context

ESP Usage Statistics* – Internally-facing Instance

- 16,000+ unique users since startup
  - 2,000+ unique users per month
  - 50,000+ notifications sent
- 1,351 Audit & Assessment Engagements
- 568 Business Processes
- 880 Metrics and Attestations for Compliance, Information Security, and Corporate Social Responsibility
  - Over 5,400 data points collected



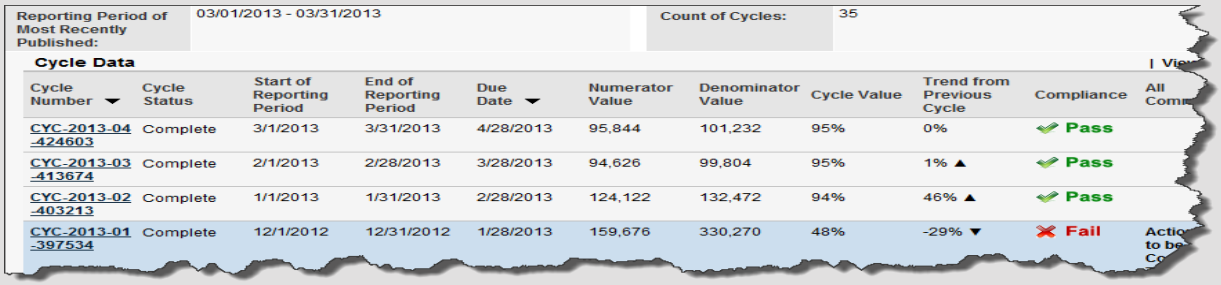
* Statistics as of 3/31/2013

Putting Risk and Compliance Decisions Into a Consistent Context

ESP Solution Portfolio:

Metrics, Evidence & Attestations

Solution Description	Realized Benefits
Delivered February, 2011 Configure and collect various types of metrics, key performance indicators (KPIs), key risk indicators (KRIs), and attestations on a recurring or ad hoc basis.	• Drove significantly higher compliance levels through transparency • Increased ability to show evidence of compliance to external auditors • Reduced the time and effort necessary to gather qualitative and quantitative compliance metrics



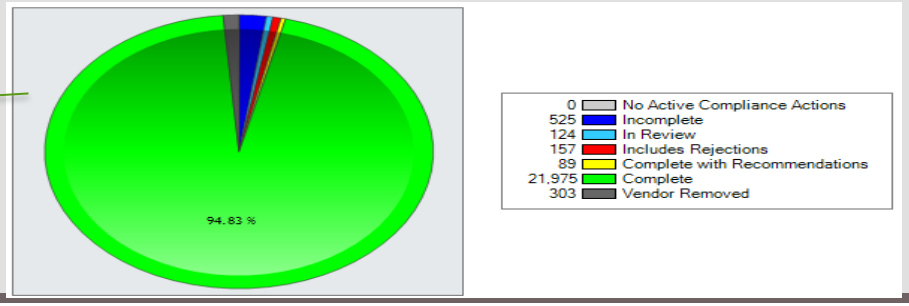
Reporting Period of Most Recently Published:	03/01/2013 - 03/31/2013			Count of Cycles:	35					
Cycle Data										
Cycle Number	Cycle Status	Start of Reporting Period	End of Reporting Period	Due Date	Numerator Value	Denominator Value	Cycle Value	Trend from Previous Cycle	Compliance	All Comm
CYC-2013-04-424603	Complete	3/1/2013	3/31/2013	4/28/2013	95,844	101,232	95%	0%	Pass	
CYC-2013-03-413674	Complete	2/1/2013	2/28/2013	3/28/2013	94,626	99,804	95%	1% ▲	Pass	
CYC-2013-02-403213	Complete	1/1/2013	1/31/2013	2/28/2013	124,122	132,472	94%	46% ▲	Pass	
CYC-2013-01-397534	Complete	12/1/2012	12/31/2012	1/28/2013	159,676	330,270	48%	-29% ▼	Fail	Actio to be Co

Putting Risk and Compliance Decisions Into a Consistent Context

ESP Solution Portfolio:
Partner Compliance Portal

Solution Description	Realized Benefits
Delivered March, 2011 Separate externally facing instance of ESP that is integrated into Humana's external portals (e.g. Provider, Pharmacy, Agent/Broker) to provide compliance training, gather required compliance attestations, and collect evidence of compliance	• Dramatically increased demonstrated compliance of downstream business partners • Reduced the time and effort necessary to manage external partner compliance

Near real-time view into third-party partner compliance attestation



Putting Risk and Compliance Decisions Into a Consistent Context

ESP Solution Portfolio:

Issue & Opportunities Management

Solution Description	Realized Benefits

Delivered December, 2010
 	
• Identify formal issues, deficiencies, opportunities or gaps found through audits and assessments
• Includes independently identified and self-identified
• Provides the business with a mechanism for prioritizing, managing, and reporting on implementation
	• Consistent company-wide process for managing issues and remediation
	• Replaced numerous ad-hoc tools for tracking issue status (13 areas)
	• Created transparency on real-time status driving significant improvement in timeliness
	  ◦ 3,882 Issue & Opportunities (IOPs) Tracked (includes historical data)
	  ◦ 3,952 Improvement Action Plans (IAPs) Tracked (includes historical data)

Putting Risk and Compliance Decisions Into a Consistent Context

ESP Solution Portfolio:

Other Modules

In Production / Near Term	In Development / Longer Term
• Engagement Management • Conflict of Interest Tracking • Enterprise Process Catalog • Continuous Compliance Activity Work Flow • Legislative and Regulatory Requirements Work Flow • Policies and Standards Work Flow • Enterprise Risk Register	• Investigation Management • Legal Hold Management • Business Continuity Planning • Incident Management • Threat and Vulnerability Management