Leveraging a GRC Platform for Compliance

Michael Cover

Manager – Blue Cross Blue Shield of Michigan

2015 - Case Study

MetricStream

GRC

SUMMIT 2015

May 11-13, 2015

ARLINGTON, VA

WASHINGTON, DC AREA

Agenda

1. Company Overview
2. Top Industry Compliance Challenges
3. Business Challenges Faced
4. Opportunity for Managing Compliance and Assurance Complexity
5. Common Framework Definitions
6. GRC Program Objectives
7. Utilizing Technology
8. Managing Implementation Risk
9. Enhanced Ongoing Support Model
10. Key Learnings and Best Practices
11. Audience Questions and Discussion

Blue Cross Blue Shield of Michigan: Company Overview

Who we are:

- A nonprofit mutual insurance company founded in 1939
- The largest health insurer in Michigan, serving 4.5 million people here and 1.3 million more in other states
- The largest network of doctors and hospitals in Michigan: 153 hospitals, and more than 30,000 doctors
- An independent licensee of the Blue Cross and Blue Shield Association
- Number of employees: more than 7,800

What we do:

- Design, sell and manage health benefit plans for individuals, families and Michigan-based employers, including:
  - Traditional plans
  - PPO (preferred provider organization) plans
  - HMO (health maintenance organization) plans
  - Wellness-based plans
  - Plans with health spending accounts
  - Dental and vision plans

Top industry compliance challenges

- Multiple regulators
- Guidance on regulations continue to emerge while development is underway
- Aggressive timeframes
- Sweeping volumes of change
- Ownership across cross functional boundaries

Business challenges faced

Opportunity Overview – The Catalyst, National Health Care Reform Compliance – Reform Critical

The passage of the Patient Protection and Affordable Care Act (PPACA) on March 23, 2010 fundamentally changed the way we do business. Payers will now essentially have the entire book of business regulated by the Center for Consumer Information & Insurance Oversight (CCIIO), a branch of Centers for Medicare and Medicaid Services (CMS).

Automated workflows and reporting are not leveraged to facilitate compliance, issue and risk transparency and are de-centralized today. Procedures and issue logs are disparate and require coordinators under executives to manually pull and monitor the information today.

Opportunity Overview - The Rationale

- From our experience with Medicare Advantage business, CMS requires strict adherence to federal regulations. We anticipate a similar oversight approach by the federal government for national health care reform.
- If **foundational elements** are established in silos other assurance and compliance area adopters may not be able to associate their governance, risk and control information within the GRC tool and ultimately enterprise-wide aggregated reporting cannot be achieved in the future.

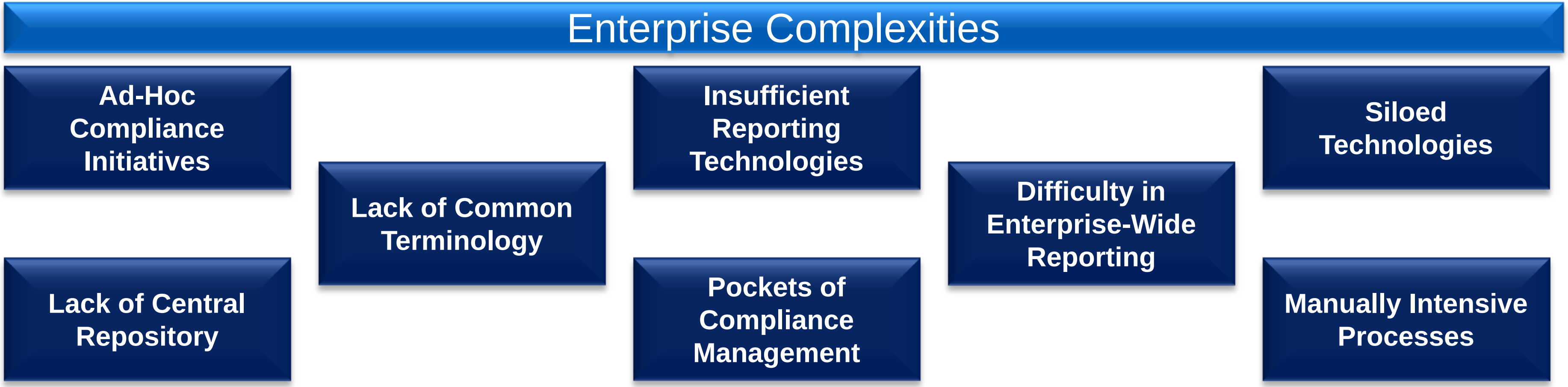
Opportunity Overview – The Risk of Not Implementing GRC

- The fines associated with PPACA alone, vary by provision, but generally is $100/member/day/provision violated
- Manually intensive national health care compliance reviews which are more daunting to the business
- Siloed solutions across the enterprise which store disparate and decentralized regulatory and control information

Opportunity for managing compliance and assurance complexity

External and internal risk and compliance management requirements are becoming increasingly complex and intrusive, while the demand for more comprehensive, consolidated and actionable governance, risk and compliance (GRC) information continues to increase.

The historic approach of managing compliance and risk in silos across different teams, processes, methods and infrastructure cannot keep up with these requirements. (Ernst Young, 2011 GRC study)



Enterprise Complexities

- Ad-Hoc Compliance Initiatives
- Lack of Central Repository
- Lack of Common Terminology
- Insufficient Reporting Technologies
- Pockets of Compliance Management
- Difficulty in Enterprise-Wide Reporting
- Siloed Technologies
- Manually Intensive Processes

Driving common framework definitions through foundational elements

Foundational Elements form a common structure for storing compliance and risk information across the organization. This common language increases reporting effectiveness and enables the organization to communicate consistently.

Organizational Structure

- Defines how the company is configured, typically guided by Organizational Charts
- May contain both functional areas and their respective high-level processes
- Drives aggregated reporting at each level of the organizational structure

Process Hierarchy

- Provides an opportunity to detail out additional functional process areas
- Helps define how monitoring activities are grouped and supports additional aggregated reporting needs

Risk Hierarchy

- Defines common risk categories at the highest level
- Risks occur at all levels and roll-up to support risk reporting which is governed by Enterprise Risk Management

Control Hierarchy

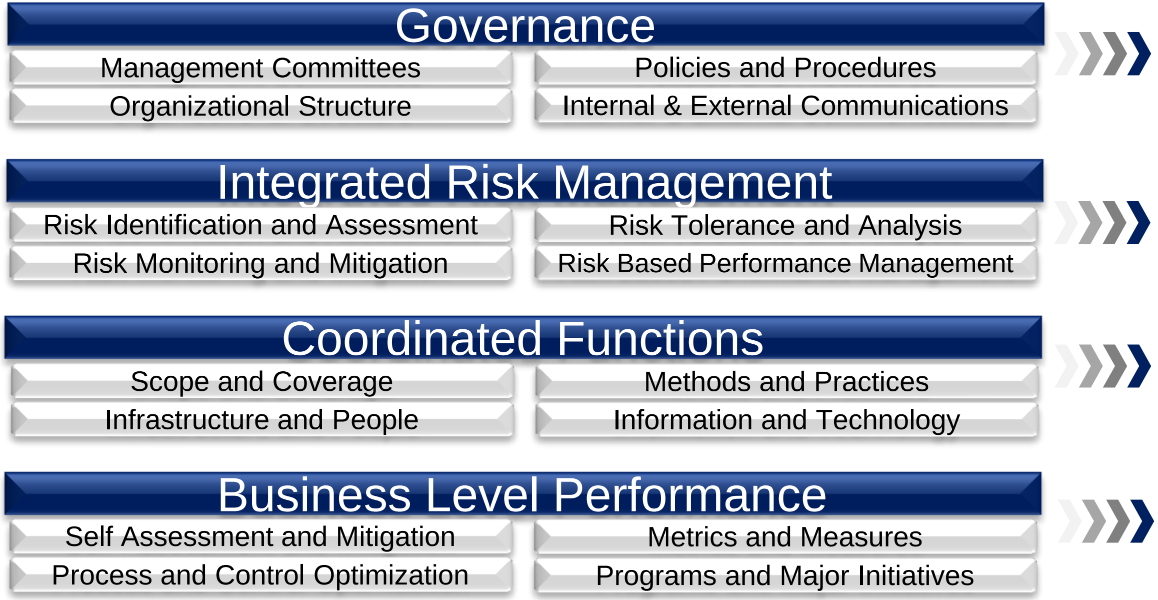
- Defines a common, consistent and standardized list of control categories across the organization
- Drives aggregated reporting across monitoring activities

Issue Hierarchy

- Defines a common, consistent and standardized way to rate issues based on identified risks or control testing
- Defines rating criteria and “severity” levels

GRC program objectives

Promote a future state vision that reduces the risk by managing corporate complexity for compliance, assurance, and business end users.



Governance

- Management Committees
- Policies and Procedures
- Organizational Structure
- Internal & External Communications

Defining the strategy and oversight responsibilities for management to drive accountability across business areas

Integrated Risk Management

- Risk Identification and Assessment
- Risk Tolerance and Analysis
- Risk Monitoring and Mitigation
- Risk Based Performance Management

Integrate risk management within the ongoing business planning and performance management processes

Coordinated Functions

- Scope and Coverage
- Methods and Practices
- Infrastructure and People
- Information and Technology

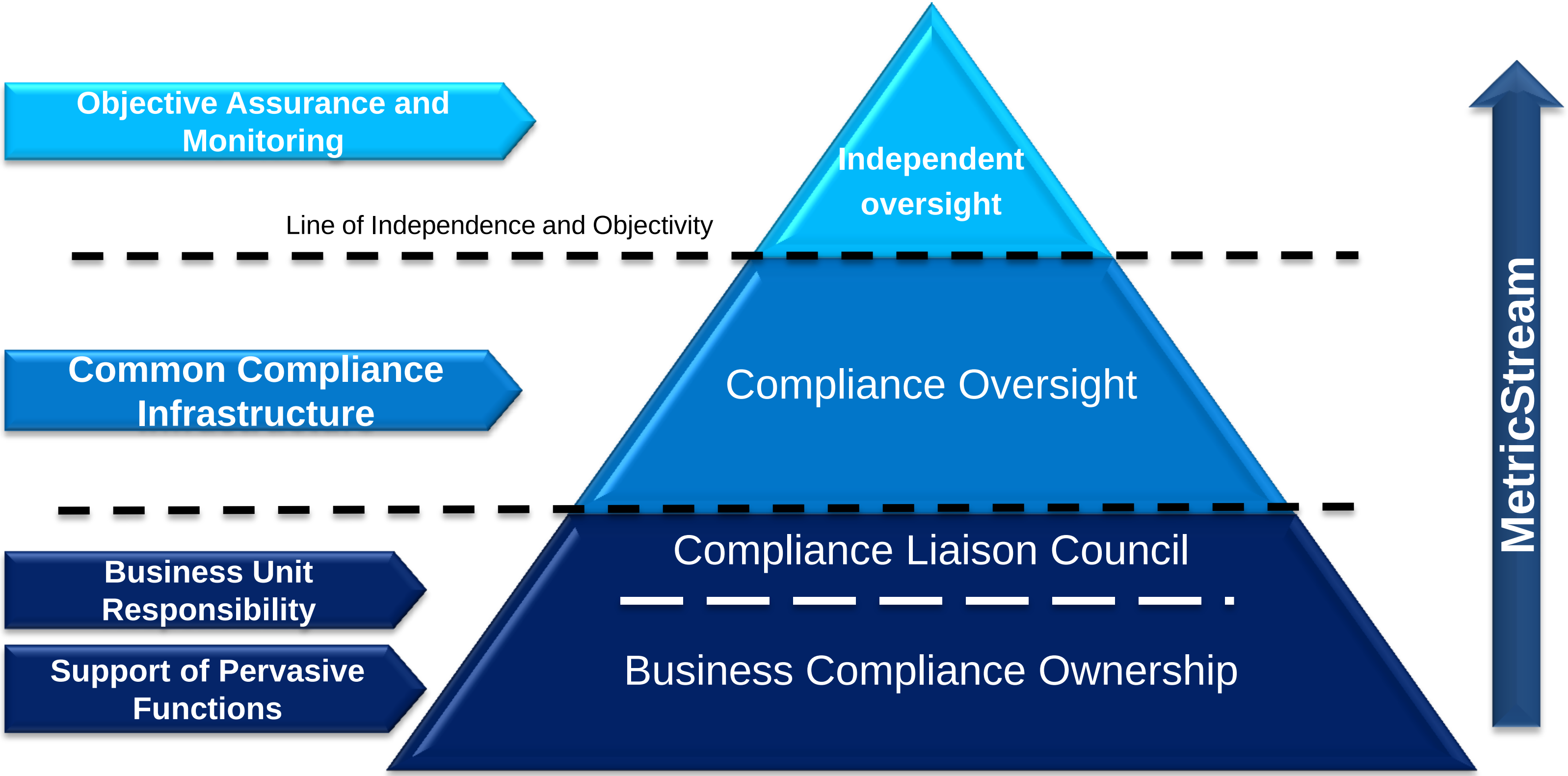
Coordinating the scope, people, processes and technology necessary to sustain an optimally effective and efficient risk management and compliance environment

Business Level Performance

- Self Assessment and Mitigation
- Metrics and Measures
- Process and Control Optimization
- Programs and Major Initiatives

Enable the organization to manage risk with optimized processes and controls at the business level

Utilizing technology to drive accountability, transparency, consistency and efficiency

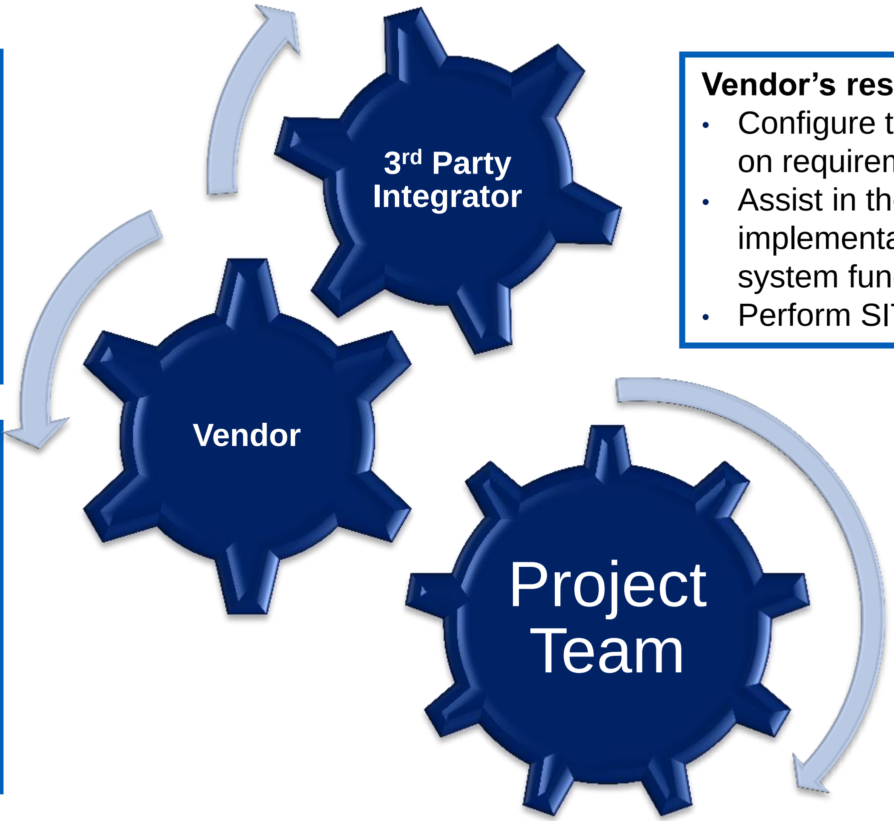

Objective Assurance and Monitoring
Line of Independence and Objectivity
Independent oversight
Common Compliance Infrastructure
Compliance Oversight
Business Unit Responsibility
Support of Pervasive Functions
Compliance Liaison Council
Business Compliance Ownership
MetricStream

Manage implementation risk through an integrated approach

MetricStream
GRC
SUMMIT 2015
May 11-13, 2015
ARLINGTON, VA

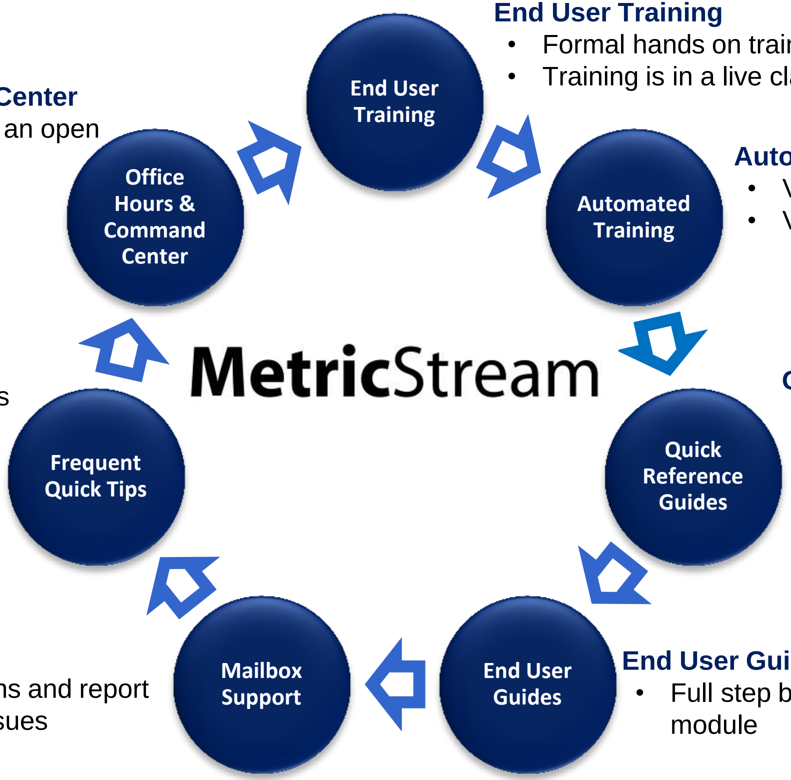
Project Team's responsibilities
- Understand business processes
- Understand system functionality
- Understand system requirements
- Assist in the configuration decisions
- Manage implementation scope
- Perform UAT testing

3rd Party Integrator's responsibilities
- Provide deep knowledge of new system business process functionality
- Help drive business process simplification
- Facilitate conference room pilots and training sessions



Vendor's responsibilities
- Configure the application based on requirements
- Assist in the design, implementation and testing of system functionality
- Perform SIT testing

Enhanced ongoing support model to support end user adoption



End User Training
- Formal hands on training sessions
- Training is in a live classroom setting

Automated Training
- Videos have been created across key topics
- Videos are about 3 minutes long

Quick Reference Guides
- Laminated desktop guides
- High level walkthrough and refresher for each module

End User Guides
- Full step by step user guides for each module

Mailbox Support
- Send questions and report application issues

Quick Tips
- Weekly quick tips and frequently asked questions from the mailbox

Office Hours & Command Center
- Weekly office hours with an open conference line

Key learnings and best practices

Key Learnings

- Align on Foundational Elements
- Define a Clear Scope
- Don’t Delay Reporting
- Increase Conference Room Pilots
- Increase Performance Testing

Best Practices

- Proof of Concept
- Leadership Buy-In
- Business Readiness
- On-Site Support
- Process Maturity
- Train Early and Often

The Road Ahead

- Module Implementations
- Additional Configuration
- Business Area Adoption
- Business Area Enablement

MetricStream
GRC
SUMMIT 2015
May 11-13, 2015
ARLINGTON, VA
WASHINGTON, DC AREA

QUESTION AND DISCUSSION

2015 - Case Study