Implementing a GRC Solution to Manage and Enhance Auditing & Monitoring

Natalie Ramello, JD, CHC
VP, Chief Compliance Officer
Rebecca Blades, CIA, CRMA, CFSA
Senior Manager Audit & Monitoring

CommunityCare

- **Home Base:** Tulsa, OK
- **Provider Owned:** Ascension St. John/Saint Francis
- **Membership:** 110,000+
- **Employees:** 425
- **Medicare Business (25%)**
  - MAPD
  - Stand-Alone PDP
- **Commercial Business (55%)**
  - Individual
  - Small Group
  - Large Group
- **ASO Self-Funded (20%)**
Governance, Risk, and Compliance (GRC)

GRC - Introduction

- Governance, risk management and compliance
- An increasingly used ‘umbrella term’ that covers these three areas of enterprise activities
- These activities are progressively being more aligned and integrated to improve enterprise performance and delivery of stakeholder needs.
RB1 Where did CMS cite this as a best practice? I didn't find it in their 2017 Program Audit and Enforcement report
Rebecca Blades, 12/16/2019
Why Implement a GRC Solution for Auditing & Monitoring?

- Visualize and communicate risk at all levels of the business.
- Develop and monitor internal controls to address risks.
- Manage the lifecycle of corporate and department level policies and procedures.
- Comply with regulations in the most efficient way possible.
- Document identified issues and their associated remediation plans.
- Enable a risk-based, business-aligned audit function.
GRC Implementation

- The integration of GRC activities within an enterprise requires a systemic approach for reliably achieving the business goals of its stakeholders.

- Such approaches are typically based on enablers of various types (e.g., principles, policies, models, frameworks, organizational structures).

GRC Implementation - Roadmap

1. Review your GRC framework to identify existing components and gaps
2. Select a GRC solution that fits your needs
   - Ensure all process owners are involved in the selection process
   - Consider both business needs and regulatory requirements
   - Review the system’s reporting capabilities
3. Select the right implementation partner
   - Consider both experience and certifications with selected GRC solution
4. Develop a feasible project timeline with key milestones
   - Include development of key reports and dashboards
   - Ensure adequate testing time and resources
5. Develop the necessary GRC procedures/workflows
   - Maintenance of policies, controls, risks, etc.
6. Train key process owners
7. Monitor GRC platform post go-live
Effective Compliance Program

CMS’ Elements of an Effective Compliance Program

- **Element I**: Written Policies, Procedures and Standards of Conduct
- **Element II**: Compliance Officer, Compliance Committee and High Level Oversight
- **Element III**: Effective Training and Education
- **Element IV**: Effective Lines of Communication
- **Element V**: Well-Publicized Disciplinary Standards
- **Element VI**: Effective System for Routine Monitoring, Auditing and Identification of Compliance Risks
- **Element VII**: Procedures and System for Prompt Response to Compliance Issues
ServiceNow GRC Overview - Key Components

- Policy & Procedure Management
- Control Management
- Risk Management
- Audit Management

Element VI: Auditing & Monitoring
CMS’ Definition for Auditing and Monitoring

Per CMS’ Compliance Program Guidelines outlined in chapter 21 of the Medicare Managed Care Manual and chapter 9 of the Prescription Drug Benefit Manual, the definitions for auditing and monitoring activities are as follows:

- **Audit** - Formal review of compliance with a particular set of standards (e.g., policies and procedures, laws and regulations) used as base measures.

- **Monitoring** - Regular reviews performed as part of normal operations to confirm ongoing compliance and to ensure that corrective actions are undertaken and effective.

Monitoring Activities - Control Record

- Control Management module used by process owners to document internal controls and classify accordingly:
  - Compliance
  - Financial Reporting
  - Operational
Monitoring Activities - Process Owner Attestations

- Control Management module used by process owners to attest to their internal controls:

<table>
<thead>
<tr>
<th>Type</th>
<th>Frequency</th>
<th>Attestation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance</td>
<td>Per Control Frequency</td>
<td>Report results of monitoring (i.e., compliance issues identified and actions taken)</td>
</tr>
<tr>
<td>Financial Reporting</td>
<td>Annually</td>
<td>Operating as intended? (Y or N)</td>
</tr>
<tr>
<td>Operational</td>
<td>Annually</td>
<td>Operating as intended? (Y or N)</td>
</tr>
</tbody>
</table>

Monitoring Activities - Tie to CMS Universe Layout

- Data from compliance control attestations is also used for CMS audit purposes.
Auditing Activities - Engagement Record

- Audit Management module used by Internal Audit to document results of audit engagements:
  - Internal Control Testing
  - Compliance Audits
    - Medicare
    - ACA

---

Auditing Activities - Tie to GRC Components

- Audit engagement record ties to risks, controls, and policies for the department/vendor being audited:
Auditing Activities - Tie to CMS Universe Layout

- Data from engagement records is also used to produce universe for CMS audit.

CPE Universe Record Layout

Element VII: Response to Compliance Issues
Tracking Issues and Remediation/Corrective Action Plans

- Issue Management module used to document issues and remediation plans for both auditing and monitoring activities:

Issues & Remediations - Tie to CMS Universe Layout

- Data from issue/remediation records also used to produce universe for CMS audit.
Element II: Compliance Officer, Compliance Committee, and High-Level Oversight

Compliance Committee Structure

- Board of Directors
- Audit & Compliance Committee of the Board
  - Executive Compliance Committee
    - Internal Audit Committee
    - Medicare Compliance Committee
Auditing & Monitoring Reporting Structure

Auditing Activities (Internal Audit)

Audit Activity performed → Document findings & request CAP → Audit Experiences → Reports, Dashboards etc. → Internal Audit Committee

Monitoring Activities (Operational Areas)

Monitoring Activity performed → Document findings & CAP → Log, Dashboards etc. → Medicare Compliance Committee

Board of Directors → Audit & Compliance Committee of the Board → Executive Compliance Committee

Example Dashboards - Auditing Activities
Example Dashboards - Monitoring Activities

Executive Level Oversight

• Real-time monitoring of risks, controls, audit engagements, issues, etc.
Key Takeaways

- Choose the right vendor for your organization.
- Develop a comprehensive roadmap for your GRC implementation.
- Review reporting capabilities prior to go-live.
- Define reasonable milestones and scope.
- Involve all relevant key process owners.
- Test, test, and test again.
- Training and document procedures.

QUESTIONS
Contact Information

Natalie Ramello  
VP Chief Compliance Officer  
natalie.ramello@utsouthwestern.edu

Rebecca Blades  
Senior Manager Audit & Monitoring  
rblades@ccok.com