Auditing & Monitoring for Health Insurers

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

CommunityCare of OK

- **Home Base:** Tulsa, OK
- **Provider Owned:** Ascension St. John/St. Francis
- **Membership:** 150,000+
- **Employees:** 500
- **2 Medicare Plans**-MAPD, MA, PDP (25%)
  - Profit
  - Non-Profit
- **Commercial Business** (55%)
  - Individual
  - Small Group
  - Large Group
- **ASO Self-Funded** (20%)

Compliance Governance

CommunityCare

Effective Compliance Program

- 1. Compliance Officer and Compliance Committee
- 2. Written Policies and Procedures
- 3. Training and Education
- 4. Effective Lines of Communication
- 5. Enforcing of Standards through well publicized disciplinary guidelines
- 6. Monitoring and Auditing
- 7. Prompt Response to detected offenses - CAP Procedure
- 8. Comprehensive Fraud and Abuse Plans – procedures to voluntarily self-report potential fraud or misconduct

CommunityCare 4

Guidance – CMS Expectations

- **30 – Overview of Mandatory Compliance Program**
- **(Chapter 21 - Rev. 109, Issued: 07-27-12, Effective: 07-20-12; Implementation: 07-20-12)**
- **(Chapter 9 - Rev. 15, Issued: 07-27-12, Effective: 07-20-12; Implementation: 07-20-12)**
- **Section 1860D-4(c)(1)(D) of the Act, 42 C.F.R. §§ 422.503(b)(4)(vi), 423.504(b)(4)(vi)**
- All sponsors are required to adopt and implement an effective compliance program, which must include measures to prevent, detect and correct Part C or D program noncompliance as well as FWA.
- The compliance program must, at a minimum, include the following core requirements:
- 1. Written Policies, Procedures and Standards of Conduct;
- 2. Compliance Officer, Compliance Committee and High Level Oversight;
- 3. Effective Training and Education;
- 4. Effective Lines of Communication;
- 5. Well Publicized Disciplinary Standards;
- 6. Effective System for Routine Monitoring and Identification of Compliance Risks; and
- 7. Procedures and System for Prompt Response to Compliance Issues.

In order to be effective, a sponsor's compliance program must be fully implemented, and should be tailored to each sponsor's unique organization, operations and circumstances.

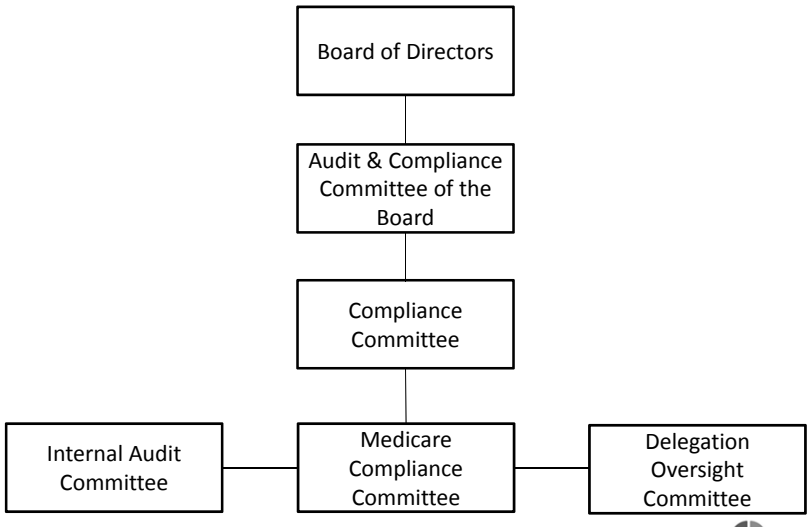
A compliance program will not be effective unless sponsors devote adequate resources to the program. Adequate resources include those that are sufficient to do the following:

1. Promote and enforce its Standards of Conduct
2. Promote and enforce its compliance program;
3. Effectively train and educate its governing body members, employees and FDRs;
4. Effectively establish lines of communication within itself and between itself and its FDRs;
5. Oversee FDR compliance with Medicare Part C and D requirements;
6. Establish and implement an effective system for routine auditing and monitoring; and
7. Identify and promptly respond to risks and findings.

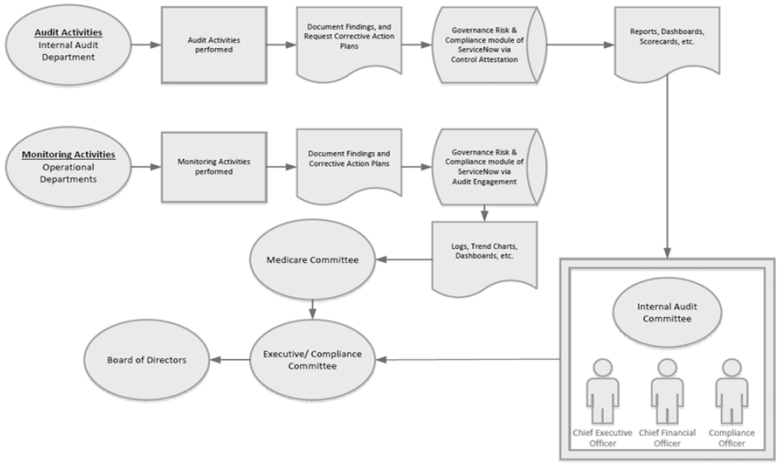
CMS will consider a sponsor's size, structure, business model, activities, the extent of its delegation of responsibilities to other entities, the breadth of its operation, and the risks it faces in evaluating whether adequate resources have been devoted to the compliance program.

CommunityCare 5

Compliance Structure



CommunityCare 6



CommunityCare

7

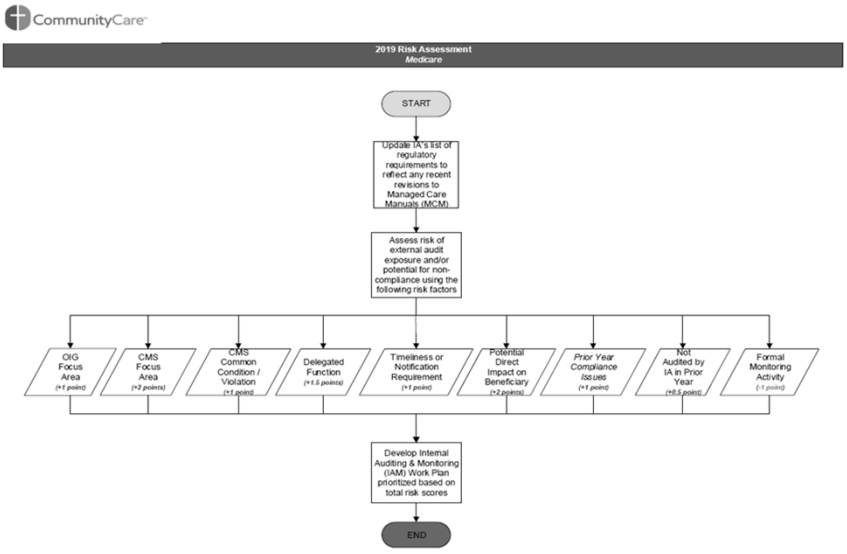
Developing A Compliance & Internal Audit Work Plan

CommunityCare

Risk Assessment

- Objective Approach
- Questionnaire
- Review Regulatory Requirements
  - Medicare Program Manuals
  - Code of Federal Regulations
- CMS/OIG Focus Areas

CommunityCare



Work Plans

2 Work Plans

- Internal Audit
  - Internal controls over financial reporting (ICOFR)
  - Internal controls over compliance
  - Compliance with Affordable Care Act rules and regulations
  - Compliance with Medicare rules and regulations
  - Compliance with URAC accreditation standards
- Compliance
  - Coding
  - High Risk Review

Internal Audit-URAC Work Plan

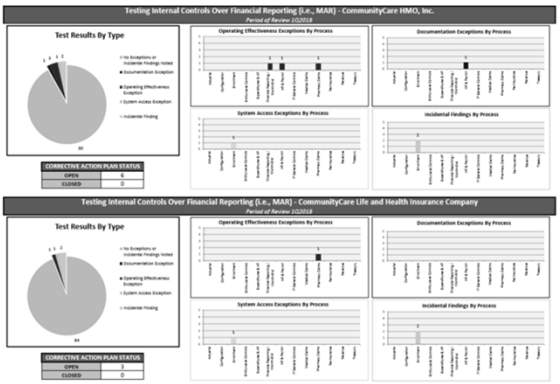
2019 Audit Schedule – Commercial Compliance (URAC)			
External Reference Number	Process	Sub-Process	Targeted Quarter for Audit
HUM 38 (Re-Audit)	Health Utilization Management	Expedited Appeal Process Time Frame	1Q
HUM 15	Health Utilization Management	Drug Utilization Management Reviewer Qualifications	2Q
HUM 16	Health Utilization Management	Prospective, Concurrent and Retrospective Drug Utilization Management	2Q
OPS 8	Health Plan Operations	P&T Formulary Development	3Q
OPS 9	Health Plan Operations	P&T Committee Membership	3Q
OPS 10	Health Plan Operations	Economic Formulary Considerations	4Q
OPS 11	Health Plan Operations	Oversight of Automated Review of Pharmacy Non-Certifications	4Q

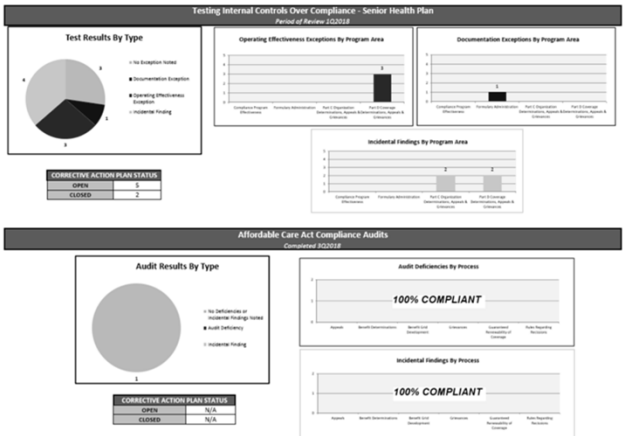
2019 Corporate Compliance Audit Work Plan and Initiatives Schedule

	SIU Coding Audit Categories	
1	Investigative Coding Audits	Q3
2	Professional Fee	Q3
3	Facility - Inpatient and Outpatient	Q3
4	Data Mining	Q4
5	Skilled Nursing Facilities, Hospice	Q4
	Key 2019 Non-Coding Audit Compliance Initiatives	
1	Revise Privacy Policies	Q1
2	Compliance Assessment of FDR Program	Q1
3	HIPAA Electronic Medical Record Access Audits	Q3
4	Implementation of HIPAA Monitoring and Detection Application	Q4
5	Revise Certain Coding and Billing Policies	Q2
6	Institutional Conflicts of Interest Policy	Q1
7	Compliance Committee Charters	Q1
8	Review of HIPAA Security Rule Policies	Q1/Q2
9	Compliance Survey	Q4
10	New Conflicts of Interest Disclosure Tracking System	Q2
11	Audit of the Gifts Policy	Q2
12	Review Accountings of Disclosure Process	Q1
13	Code of Excellence Review	Q4
14	Employee Compliance Training Test Review	Q2
15	New Employee Conflicts of Interest Forms	Q2
16	Data Mining Tool	Q4
17	HIPAA Security Awareness	Q2
18	Government Investigations/Audit Policy	Q2
19	Code of Excellence Certifications	Q4
20	Pharmacy Benefit Manager Review	Q3
21	Transportation Providers Checklist Review	Q2
22	Business Associate Audits	Q3

CommunityCare

Audit Dashboard





CommunityCare

Monitoring Activities

CommunityCare

Auditing v. Monitoring

- **Auditing:** formal reviews usually by the internal audit or compliance department against applicable standards (e.g. policies and procedures, law and regulations).
- **Monitoring:** regular reviews performed by various departments as part of normal operations to confirm ongoing compliance with applicable requirements. These activities also ensure that corrective actions are undertaken and effective.

What is Internal Monitoring?

A process within an organization to provide reasonable assurance regarding:

- The reliability and integrity of information
- Compliance with policies, plans, procedures, laws and regulations
- The safeguarding of assets
- The efficient use of resources
- The accomplishment of established objectives and goals of operations and programs

Why is Internal Monitoring Important?

Outside of the CMS Requirement, an effective monitoring program:

- 1) Provides early identification of weaknesses and risks.
- 2) Engages associates throughout the organization.
- 3) Sets the right tone for your organization with associates and the public.

Keep In Mind

- In our experience, we have found that many employees often have unexpressed anxiety and fear about the auditing and monitoring and what non-compliance may be uncovered.
- Positive communication and setting realistic expectations will allow everyone to be engaged, actively participate, accept the findings and implement change.

Monitoring & Operations

For an effective and ongoing Internal Monitoring Program, the Compliance Teams must:

- Organize the approach
- Identify the internal controls and potential risk areas for monitoring
- Set clear and reasonable expectations for the operational teams involved.
- Explain how to capture, document and report non-compliance. • Identify the path to corrective actions.

Determining What to Monitor

- Review Risk Assessment?
- Do you know of potential issues?
- Are there indications of problems that might need closer scrutiny?
- Which areas have had critical audit findings in the past?

CMS Common Conditions | Delegated Vendor Responsibilities | OIG Work Plan | Previous Audit Findings | Newly Published P&Ps

Developing a Monitoring Plan

- **Identify the Teams, Monitoring Areas and Reporting Responsibilities**

Who will do what task	What was done well	Approval
Deliverable deadlines	Areas of improvement	Implementation
Delivery Methods	Effectiveness of the activity	Repeat Monitoring
Delivery Expectations	Moving forward activities	Reporting Findings

Don't forget to consider competing priorities/projects for the operational teams. You want buy-in and long term commitment!

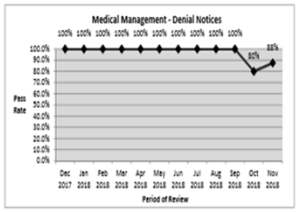
2019 MEDICARE MONITORING SCHEDULE BY DEPARTMENT				
Department	Name of Component / Operation	Description of Monitoring Activity	Control / Monitoring Frequency	
Behavioral Health	Denial Notices	Verify denial notices are timely, accurate and contain sufficient detail to explain the reason for denial.	Monthly	
Behavioral Health	Organization Determinations	Confirm that pre-service authorization requests have been processed in a timely manner.	Monthly	
Behavioral Health	Provider Outreach	Verify sufficient outreach to providers or enrollees was performed to obtain additional information necessary to make appropriate clinical decisions.	Monthly	
Claims	Contracted Provider Claims	Ensure contracted provider claims are being processed timely.	Weekly	
Claims	Member Denial Letters	Denial notices are timely, accurate and contain sufficient detail to explain the reason for denial.	Weekly	
Claims	Member Reimbursements	DMR requests are processed timely and accurately.	Weekly	
Claims	MSP vs MMR Reconciliation	Review the MSP vs MMR files provided by DAR monthly to verify if claims were paid properly based on the information in our system. Any discrepancies are verified by the COB Specialist and refunds requested as necessary.	Monthly	
Claims	Non-Contracted Provider Claims	Non-contracted provider claims are processed timely.	Weekly	
Claims	OIG/GSA Exclusions	Review monthly reports from Data Analysis & Reporting and request refunds for all non-emergent claims paid to excluded providers and all non- urgent and emergent claims paid to opted out providers.	Monthly	
Claims	Provider Waiver of Liability Letters	Denial notices contain a copy of the Waiver of Liability form or a link to the form.	Weekly	
Compliance	Annual CPE Audit	The annual Medicare CPE audit is conducted by an independent party, and the audit results are shared with the governing body.	Annually – Dec	

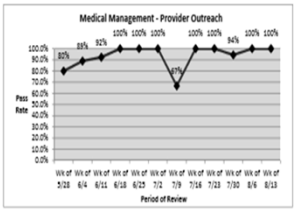
CommunityCare

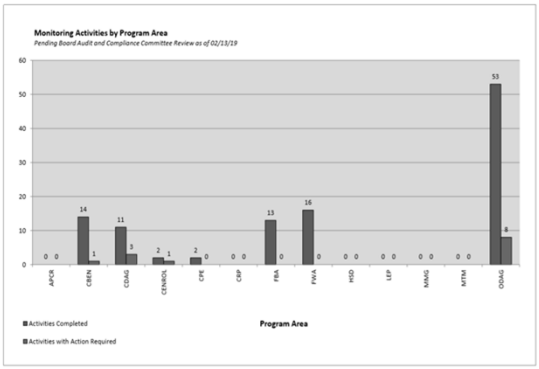
Monitoring Dashboard

High Risk Areas

ODAG - Part C Organization Determinations, Appeals & Grievances







Program Area	Program Area Description	# of Activities Completed	# of Activities w/ Action Required		
			High Risk	Medium Risk	Low Risk
APCR	Application Procedures & Contract Requirements	0			
CBEN	Part C Benefits & Beneficiary Protections	14		1	
CDAG	Part D Coverage Determinations, Appeals & Grievances	11	3		
CENROL	Enrollment & Disenrollment	2		1	
CPE	Compliance Program Effectiveness	2			
CRP	Part C Relationships with Providers	0			
FBA	Formulary Benefit Administration	13			
FWA	Fraud, Waste & Abuse	16			
HSD	Health Service Delivery (Network Adequacy)	0			
LEP	Creditable Coverage Determinations & Late Enrollment Penalty	0			
MMG	Medicare Marketing Guidelines	0			
MTM	Medication Therapy Management	0			
ODAG	Part C Organization Determinations, Appeals & Grievances	53		8	
		111	**3**	**10**	**0**

CommunityCare

First Tier, Downstream & Related Entities

FDR Compliance Oversight

- Covered Entities are ultimately responsible for actions delegated to first tier, downstream, and related (FDR) entities
- Entities must maintain adequate and effective oversight of the FDR & Vendors/Subcontractors to ensure that they comply with applicable contractual and regulatory requirements

CMS Language

It is critical that sponsors correctly identify those entities with which they contract that qualify as FDRs. Sponsors are required to comply with CMS requirements for FDRs. Unless it is very clear that an entity is or is not an FDR, the determination of FDR status requires an analysis of all of the circumstances. Sponsors should have clearly defined processes and criteria to evaluate and categorize all vendors with which they contract."

Evaluation of Core Services

- When evaluating entities for enrollment in your network its important to determining whether an entity is an FDR, for the purpose of exercising compliance and operational oversight
  - Whether the entity performs a core service
  - Whether the function is a service the Covered Entity is required to do or provide under its contract with Medicare and applicable federal regulations or guidance
  - Whether the function directly impacts enrollees
  - Whether the entity has interaction with enrollees
  - Whether the entity has access to beneficiary information or personal health information
  - Whether the entity has decision-making authority
  - Whether the function places the entity in a position to commit health care fraud, waste or abuse
  - The risk that the entity could harm enrollees or violate Medicare and/or other regulatory program requirements

FDRs: Who is a First Tier Entity?

- First Tier Entity - A party that enters into a written arrangement with a Medicare Advantage Organization ("MAO") or Part D plan sponsor to provide:
  - Administrative services (e.g., marketing, utilization management, quality assurance, applications processing, enrollment and disenrollment functions, claims processing, adjudicating Medicare organization determinations, appeals and grievances, provider credentialing); or
  - Health care services to a Medicare eligible individual under the Medicare Advantage program or Part D program (e.g., independent practice association, hospital, PHO)
  - Examples: Independent Practice Associations, Call Center, Credentialing, Field Marketing Organization & PBM

FDRs: Who is a Downstream Entity?

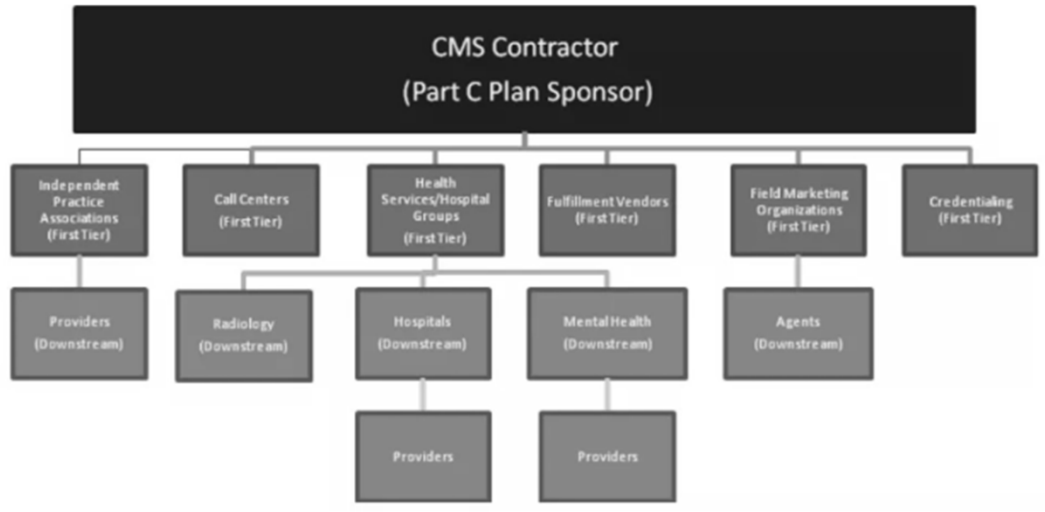
- Downstream Entity – A party that enters into a written arrangement with a First Tier entity for the provision of administrative services or health care services to a Medicare eligible individual under the Medicare Advantage program or Part D program
  - Hospital within a health system that has entered into a system level agreement
  - Credentialing verification organization
  - Examples: Providers, Radiology, Hospitals, Mental Health Agents

FDRs: Who is a Related Entity?

- Related Entity - Any entity that is related to the sponsor by common ownership or control and either: (1) performs some of the sponsor's management of functions under a contract of delegation; (2) furnishes services to Medicare enrollees under an oral or written agreement; or (3) leases real property or sells materials to the sponsor at a cost of more than $2,500 during a contract period

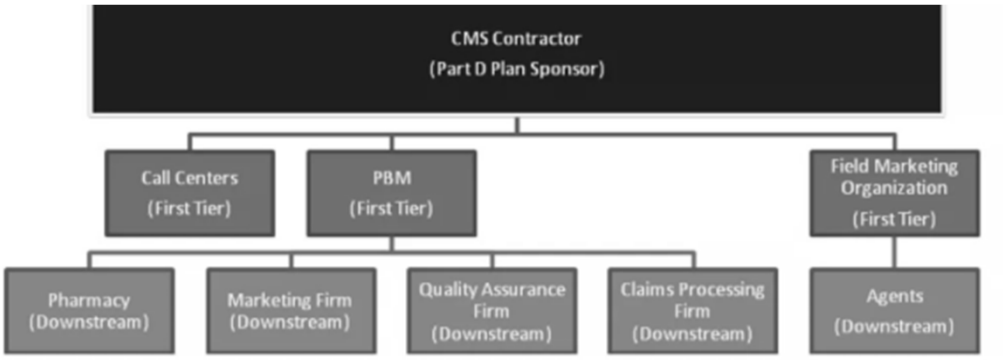
CommunityCare 31

Part C



CommunityCare 32

Part D



FDR Spotting: CMS' Factors To Consider

- Impact on enrollees
- Extent of interaction with enrollees (orally or written)
- Access to PHI
- Decision-making authority

7 Steps to FDR Success

- 1. Develop Governance Structure & Program Objectives
- 2. Assign Roles and Responsibilities
- 3. Inventory Vendors and Identify FDRS
- 4. Perform Risk Assessments
- 5. Prepare and Determine Methodology
- 6. Evaluate and Audit
- 7. Report Results and Ongoing Monitoring

What are FDRs Required to Do?

- Regulatory (and Organizational) Expectations
  - Sponsors/FDRs need to exercise oversight of subcontractor's compliance efforts (e.g., vendor management program), if Part C/D administrative, management or clinical functions are delegated
  - FDRs must maintain an effective compliance program that meets the compliance program requirements for Medicare Part C/D plans
  - FDRs much have systems in place to train employees regarding FWA (if no deemed status) and general compliance (e.g., standards of conduct, HIPAA)
  - FDRs must investigate, correct and document all instances of suspected non-compliance

Pre-Delegation Assessment

- Prior to delegating a core service to an FDR, the Covered Entity should perform a pre-delegation assessment
  - The review will cover topics such as the FDR's experience in the delegated area, its operational performance, policies and procedures, compliance program infrastructure and adherence, compliance monitoring and auditing, HIPAA Privacy and Security, record retention, and reportable metrics
  - In determining whether to conduct the review, the Covered Entity should assess the FDR's specific functions, the risks associated with the FDR, and the size and magnitude of the contract

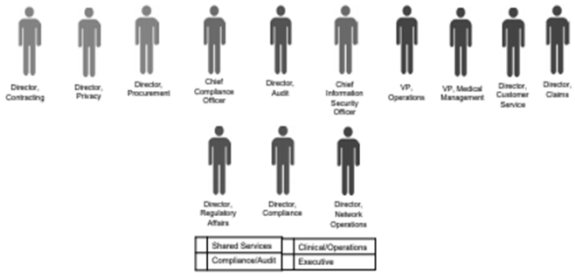
Annual Audit

- Audit
  - Onsite review is conducted and evidence is evaluated using standardized audit tools.
  - Interviews take place with focus on internal processes.
- Post Audit
  - Corrective action plans are issued for deficiencies identified during the annual review.
  - Continuous oversight, monitoring and follow-up occurs through monthly and quarterly reports.

FDR Oversight

- Ensures that proper internal controls are in place to monitor FDRs on a routine basis
- Review FDR performance to ensure compliance with:
  - •Contractual provisions
  - Policies and procedures
  - •CMS requirements, applicable state and federal regulatory requirements
  - •Accreditation standards
  - •Oversight of downstream entities used by FDR
- Provides management with reasonable assurance that delegates are delivering quality services on behalf of the organization

Delegation Oversight Committee



ROLE	RESPONSIBILITY
Committee	Approve recommendations, assist with prioritization, review audit results and decide on action
Audit Team	Develop tool, conduct audit, summarize results, make recommendations to oversight committee
Business Owner	Provide functional standards and requirements, assist in development of tool, participate in on sight audit as needed
Other SMEs	IT-Perform audit on technical safeguards

Additional Resources

- Chapter 21-Medicare Managed Care Manual
- Chapter 9-Prescription Drug Benefit Manual
- For more information on requirements for contracts with FDRs, see Pub. 100-16, Medicare Managed Care Manual, chapter 11, §110.

Implementing a GRC Platform
Automating Audit & Monitoring Activities

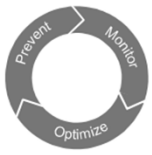
GRC

- Governance, risk management and compliance
- An increasingly used 'umbrella term' that covers these three areas of enterprise activities
- These areas of activity are progressively being more aligned and integrated to improve enterprise performance and delivery of stakeholder needs.
- GRC Solution is a CMS cited Best Practice (2017 Program Audit)

CommunityCare 43

GRC-Definition and Key Components

GRC is a comprehensive term to describe the organizational approach covering Governance, Risk and Compliance areas:



Key Components

Business Controls:
- Automated Controls (Configuration)
- Semi-Automated Controls (Reports/Transactional Analysis)
- Manual controls (Policies)

Security:
- Access to sensitive functions
- Segregation of Duties
- Access management process

Business Risk (Operational/Industry/regulation):
- KPI
- KRI

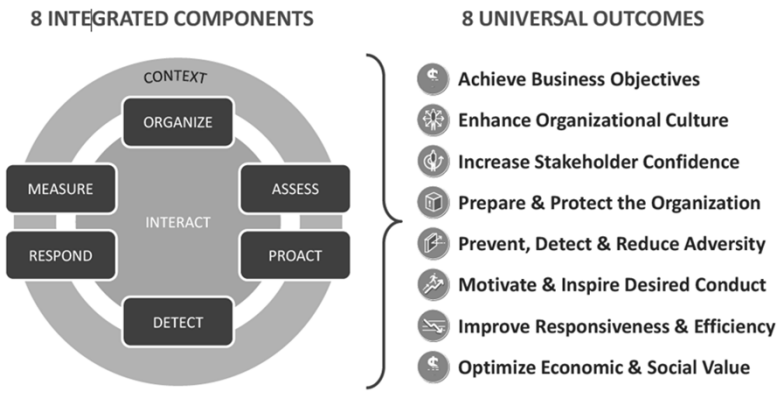
Compliance Framework
- Policy Management
- Work Papers
- Certification Process
- Dashboards

CommunityCare 44

Implementing Governance

- The integration of the implementation of the 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).

A GRC Model



Why Implement a GRC Solution?

- Manage the lifecycle of corporate policies and their exceptions.
- Comply with regulations in the most efficient way possible.
- Visualize and communicate risk at all levels of the business.
- Investigate and resolve cyber and physical incidents.
- Centralize business continuity and disaster recovery planning.
- Enable risk-based, business-aligned internal audit.

CommunityCare 47

CommunityCare 48

CommunityCare 49

Key Takeaways

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

CommunityCare 50

Enterprise Risk Management

Fitting the Puzzle Pieces Together to Reduce Risk

CommunityCare

What is ERM?

Enterprise Risk Management (ERM) is defined by the Committee of Sponsoring Organizations (COSO) as “a process, effected by an entity’s board of directors, management and other personnel, applied in strategy-setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.”

Why ERM Is Important

Underlying Principles:

- Every entity, whether for-profit or not, exists to realize value for its stakeholders.
- Value is created, preserved, or eroded by management decisions in all activities, from setting strategy to operating the enterprise day-to-day.

Key Implementation Factors

1. Organizational design of business
2. Establishing an ERM organization
3. Performing risk assessments
4. Determining overall risk appetite
5. Identifying risk responses
6. Communication of risk results
7. Monitoring
8. Oversight & periodic review by management

ERM…

- Provides a comprehensive and systematic approach to more proactive and holistic risk management
- Provides a common lexicon of risk terminology, and provides direction and guidance for implementing ERM
- Requires that organizations examine their complete portfolio of risks, consider how those risks interrelate, and that management develops an appropriate risk mitigation approach to address these risks in a manner that is consistent with the organization's strategy and risk appetite

QUESTIONS

Contact Information

Natalie Ramello
VP Chief Compliance & Risk Officer
nramello@ccok.com

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

CommunityCare

57