Health Plan Compliance Risk Assessment

Identify and Manage
Compliance Risks Effectively

Ginete Healthcare Consulting Group
hello@ginete.co | ginete.co
(818) 308-5476

2025 Edition

Table of Contents

1. Introduction to Compliance Risk Assessment

Compliance risk assessment is a systematic process for identifying, evaluating, and prioritizing regulatory compliance risks faced by health plan organizations. CMS requires Medicare Advantage and Part D sponsors to conduct annual risk assessments as part of their compliance program obligations.

Purpose and Benefits

- Identify areas of highest compliance risk before violations occur
- Allocate limited compliance resources to greatest areas of need
- Inform the annual compliance audit work plan
- Demonstrate proactive compliance program management to regulators
- Support Board and leadership oversight of compliance risks
- Track risk trends and program effectiveness over time

Regulatory Requirements

- CMS Compliance Program Guidelines (Chapter 9/21) require risk assessment
- OIG Compliance Program Guidance recommends systematic risk analysis
- NCQA accreditation standards expect risk-based compliance planning
- State Medicaid contracts often require annual risk assessments
- 42 CFR 438.608 requires Medicaid MCO compliance risk identification

2. Risk Assessment Framework

An effective compliance risk assessment framework provides a structured, repeatable methodology for evaluating risks across the organization.

Framework Components

- Risk Universe: Comprehensive inventory of all compliance risk areas
- Risk Identification: Methods to discover and document potential risks
- Risk Analysis: Evaluate likelihood and impact of each risk
- Risk Scoring: Quantify and rank risks using consistent methodology
- Risk Response: Develop mitigation strategies for priority risks
- Risk Monitoring: Ongoing tracking and reassessment

Risk Assessment Methodology

- Inherent Risk: Risk level without considering existing controls
- Control Effectiveness: How well current controls mitigate the risk
- Residual Risk: Remaining risk after controls are applied
- Risk Appetite: Organization's tolerance for residual risk
- Risk Response: Accept, mitigate, transfer, or avoid

Data Sources for Risk Assessment

- Prior audit findings (internal and external)
- CMS enforcement actions and industry trends
- Compliance hotline reports and investigations
- Operational monitoring data and performance metrics
- Regulatory changes and new requirements
- Organizational changes (new products, markets, leadership)
- FDR performance data and audit results

3. Identifying Compliance Risks

Risk Identification Methods

- Regulatory scanning: Monitor new/changed CMS requirements
- Internal interviews: Meet with operational leaders across departments
- Data analysis: Review operational metrics for compliance indicators
- Industry benchmarking: Compare performance to peers
- External intelligence: CMS audit findings, OIG reports, enforcement trends
- Incident review: Analyze prior compliance events and near-misses

Key Questions to Ask

- What regulatory requirements apply to this area?
- What could go wrong? What are the failure modes?
- What has gone wrong before (internally or at other organizations)?
- What controls exist? How effective are they?
- What would the impact be if a violation occurred?
- Have there been regulatory changes affecting this area?
- Are there new products, populations, or markets increasing risk?

Stakeholder Input

- Compliance Officer and staff observations
- Medical Director and clinical leadership insights
- Operations leaders (claims, enrollment, member services)
- Legal counsel perspective on regulatory developments
- Internal audit findings and recommendations
- Board and executive concerns

4. Risk Scoring and Prioritization

Likelihood Assessment

Rate the probability that a compliance risk event will occur:

- 5 - Almost Certain: Expected to occur in most circumstances
- 4 - Likely: Will probably occur in most circumstances
- 3 - Possible: Might occur at some point
- 2 - Unlikely: Could occur but not expected
- 1 - Rare: May occur only in exceptional circumstances

Impact Assessment

Rate the severity of consequences if the risk event occurs:

- 5 - Critical: Contract termination, major CMP, significant member harm
- 4 - Major: Enrollment sanctions, substantial CMP, reputational damage
- 3 - Moderate: CAP required, moderate penalties, operational disruption
- 2 - Minor: Warning letter, minor operational impact, limited exposure
- 1 - Negligible: Internal correction only, minimal external consequence

Risk Score Matrix

Risk Score = Likelihood x Impact. Scores range from 1-25:

- Critical (20-25): Immediate action required, executive attention
- High (12-19): Priority mitigation, regular leadership reporting
- Medium (6-11): Planned mitigation, routine monitoring
- Low (1-5): Accept or monitor, address opportunistically

Control Effectiveness Rating

- Strong: Controls well-designed, operating effectively, regularly tested
- Adequate: Controls in place, generally effective, some gaps
- Weak: Controls exist but have significant gaps or inconsistent operation
- None: No meaningful controls in place for this risk

5. Key Risk Areas for Health Plans

High-Impact Risk Areas

- Coverage determinations and appeals timeliness
- Marketing and sales compliance (especially TPMO oversight)
- Provider network adequacy and directory accuracy
- Claims processing accuracy and timeliness
- Data privacy and security (PHI protection)
- Risk adjustment data accuracy (RADV exposure)
- Formulary and pharmacy benefit administration

Operational Risk Areas

- Member enrollment and disenrollment processing
- Grievance and complaint handling
- Credentialing and provider contracting
- Care coordination and transitions of care
- Quality measure data collection and reporting
- Member communication accuracy and timeliness

Emerging Risk Areas

- Telehealth and virtual care compliance
- Health equity and non-discrimination requirements
- AI/ML use in utilization management decisions
- Social determinants of health data privacy
- Interoperability and data sharing requirements
- Cybersecurity and ransomware threats to operations

6. First-Tier, Downstream, and Related Entity (FDR) Risks

Health plans are responsible for the compliance of their delegated entities. FDR oversight is consistently identified as a high-risk area in CMS audits.

FDR Risk Categories

- PBM (Pharmacy Benefit Manager) compliance with Part D requirements
- Delegated utilization management vendors
- Claims processing and payment accuracy
- Marketing organizations (FMOs, TPMOs, agents/brokers)
- Provider groups with delegated credentialing or UM
- Care management and disease management vendors
- Technology vendors with access to PHI

FDR Oversight Requirements

- Written delegation agreements with compliance provisions
- Pre-delegation assessment of FDR capabilities
- Annual FDR compliance training and attestation
- Ongoing performance monitoring and reporting
- Regular auditing of delegated functions
- Corrective action authority and enforcement
- OIG/GSA exclusion list screening for FDR workforce

Assessing FDR Risk

- What functions are delegated and how critical are they?
- Does the FDR have a compliance program?
- What is the FDR's audit history and compliance track record?
- How many members/transactions are affected by this FDR?
- Are there sub-delegations adding complexity?
- What monitoring data is the plan receiving and reviewing?

7. Developing Risk Mitigation Strategies

Mitigation Approaches

- Process improvements: Redesign workflows to prevent errors
- Technology solutions: Automation, alerts, and monitoring tools
- Training: Targeted education on high-risk areas
- Policy updates: Strengthen written standards and procedures
- Staffing: Adequate resources for compliance-critical functions
- Oversight: Enhanced monitoring and reporting for priority risks

Corrective Action Planning

- Define specific, measurable corrective actions for each priority risk
- Assign accountable owners with authority to implement changes
- Establish realistic timelines with interim milestones
- Identify resource requirements and secure commitment
- Define success metrics and validation methods
- Plan for sustainment after initial correction

Risk Acceptance

Some residual risks may be accepted after appropriate analysis and approval:

- Risk must fall within organizational risk appetite
- Cost of further mitigation exceeds expected benefit
- Documented approval by appropriate authority level
- Ongoing monitoring to detect changes in risk level
- Regular reassessment of acceptance decisions

8. Monitoring and Reporting

Ongoing Monitoring Activities

- Key Risk Indicators (KRIs) tracked monthly/quarterly
- Compliance dashboards with red/yellow/green status
- Operational metrics tied to compliance performance
- Regulatory change tracking and impact assessment
- FDR performance reports and trend analysis
- Compliance incident and investigation tracking

Reporting to Leadership

- Quarterly risk assessment updates to Compliance Committee
- Annual comprehensive risk report to Board of Directors
- Immediate escalation of critical or emerging risks
- Trending data showing risk movement over time
- Mitigation progress and effectiveness reporting

Risk Register Maintenance

- Living document updated throughout the year
- New risks added as identified
- Risk scores updated based on new information
- Mitigation status tracked and reported
- Closed risks archived with resolution documentation

9. Annual Risk Assessment Process

Step-by-Step Annual Process

- Step 1: Review prior year risk assessment and outcomes
- Step 2: Update risk universe based on organizational changes
- Step 3: Gather data from internal/external sources
- Step 4: Conduct stakeholder interviews and workshops
- Step 5: Score risks using consistent methodology
- Step 6: Validate results with operational leaders
- Step 7: Develop/update mitigation plans for priority risks
- Step 8: Present findings to Compliance Committee and Board
- Step 9: Develop annual audit work plan based on risk priorities
- Step 10: Implement monitoring and reassessment schedule

Timing and Integration

- Complete annual risk assessment in Q4 for following year planning
- Align with annual compliance audit work plan development
- Integrate with organizational strategic planning cycles
- Coordinate with enterprise risk management if applicable
- Update for significant mid-year changes (new regulations, events)

10. Risk Assessment Tools and Templates

Essential Tools

- Risk Register: Central repository of all identified risks with scores
- Risk Heat Map: Visual display of risks by likelihood and impact
- Risk Scoring Matrix: Consistent methodology for evaluation
- Stakeholder Interview Guide: Structured questions for risk identification
- Control Assessment Worksheet: Evaluate existing mitigations
- Mitigation Action Plan: Track corrective actions and timelines

Best Practices

- Use consistent scoring methodology across all risk areas
- Involve operational leaders - they know the risks best
- Consider both current risks and emerging/future risks
- Document assumptions and rationale for risk scores
- Calibrate scores across assessors for consistency
- Keep it practical - focus on actionable insights, not perfection

Need help conducting your compliance risk assessment? Contact Ginete Healthcare Consulting Group:
Email: hello@ginete.co | *Phone: (818) 308-5476* | *Web: ginete.co*

Disclaimer: This guide is provided for informational purposes only and does not constitute legal advice. Regulatory requirements are subject to change. Organizations should consult with qualified legal counsel and compliance professionals for guidance specific to their circumstances.