PYA Healthcare Regulatory Roundup #103 – Compliance Risk Assessments: Building Blocks for Your Annual Plan

Presented October 15, 2025 by PYA's Shannon Sumner and Rhonda Buckholtz | Part of the Healthcare Regulatory Roundup Webinar Series

https://www.pyapc.com/insights/hcrr-103-webinar-compliance-risk-assessments-building-blocks-for-your-annual-plan/

Please note, this transcript was generated automatically. PYA cannot guarantee its accuracy or completeness.

WEBINAR SUMMARY

This episode of PYA's Healthcare Regulatory Roundup focused on building compliance programs, risk assessments, and annual plans. Shannon Sumner and Rhonda Buchholz emphasized the importance of leadership commitment, a culture of compliance, and continuous training. They discussed risk identification, prioritization, and documentation, highlighting the need for comprehensive and dynamic risk assessments. Key risks for 2026 include cybersecurity, data privacy, regulatory changes, and vendor management. The Office of the Inspector General (OIG)'s *Compliance Program Guidance*, the Department of Justice (DOJ)'s *Evaluation of Corporate Compliance Programs*, and The Committee of Sponsoring Organizations' (COSO's) *Enterprise Risk Management Framework* were recommended resources.

Key topics include:

- **Compliance risk assessments**
- **Annual compliance plan**
- **Regulatory compliance requirements**
- **Ethical decision making**
- **Leadership commitment to compliance**
- **Compliance culture**
- **Compliance training and education**
- **Auditing and continuous monitoring for compliance**
- **Corrective actions**
- **Compliance risk identification, prioritization, and documentation**
- **Alternative payment models**
- **AI-enabled medical devices and cybersecurity**
- **340B program and compliance**
- **OIG's *Compliance Program Guidance***
- **DOJ's *Evaluation of Corporate Compliance Programs* (September 2024)**
- **COSO *Enterprise Risk Management Framework***

WEBINAR HIGHLIGHTS AND FREQUENTLY ASKED QUESTIONS

What is the purpose of a compliance risk assessment in healthcare?

- A compliance risk assessment identifies areas of potential noncompliance within a healthcare organization, helping leaders prioritize resources, improve internal controls, and align compliance initiatives with strategic and operational goals.
- It also demonstrates a proactive approach to regulatory expectations set by the OIG and DOJ.

How often should a healthcare organization conduct a compliance risk assessment?

- At minimum, a compliance risk assessment should be conducted annually, with continuous monitoring and updates throughout the year as regulations, technologies, and operations change.
- The assessment should remain a living document rather than a one-time project.

Who should participate in the compliance risk assessment process?

- Effective risk assessments require input from multiple stakeholders including compliance officers, clinical leadership, revenue cycle and billing teams, IT and security, human resources, legal counsel, and executive leadership.
- The OIG recommends that the Compliance Committee coordinate joint risk assessments with audit and risk management teams.

What internal and external risks should be included in a compliance risk assessment?

- Internal risks often include billing and coding errors, data privacy lapses, inadequate training, or gaps in documentation.
- External risks include evolving regulations, OIG Work Plan updates, DOJ enforcement actions, payer policy changes, and industry benchmarking data.

How can organizations build and maintain a compliance risk inventory?

- A risk inventory should include each risk's description, regulatory citation, source, risk owner, and mitigation status.
- The document should be updated quarterly or semiannually and reviewed by compliance leadership to ensure emerging risks are captured).

What tools or frameworks support effective compliance risk management?

- Key resources include:
  - OIG's *Compliance Program Guidance*, found at: https://oig.hhs.gov/compliance/general-compliance-program-guidance/
  - DOJ's *Evaluation of Corporate Compliance Programs* (September 2024), found at: https://www.justice.gov/criminal/criminal-fraud/page/file/937501/dl?inline=)
  - COSO *Enterprise Risk Management Framework*, found at: https://www.coso.org/erm-framework
- Together, these resources define risk accountability, methodology, and continuous improvement practices.

How can healthcare leaders prioritize risks effectively?

- Prioritization uses scoring criteria such as likelihood, impact, regulatory sensitivity, readiness, and reputational harm.
- Risks scoring highest across these dimensions should be addressed first, while others are monitored or scheduled for future action.

What are the top compliance risks healthcare organizations should prepare for in 2026?

- Emerging priorities include:
  - Cybersecurity and data privacy
  - Artificial intelligence (AI) in healthcare
  - Vendor and third-party risk management
  - 340B program
  - Quality of care in post-acute settings
  - Regulatory impacts of the OBBBA and other federal reforms

What role does leadership play in compliance success?

- Leadership must model a culture of ethics and accountability, allocate sufficient resources, and integrate compliance objectives into performance evaluations.
- Without executive support, compliance programs risk becoming underfunded or ignored.

Why is continuous training essential for compliance effectiveness?

- Training ensures staff understand both regulatory obligations and the "why" behind compliance policies.
- Scenario-based and role-specific education that is documented for auditing purposes reduces errors, encourages reporting, and sustains a culture of compliance over time.

ACTION ITEMS

- Establish a Compliance Committee subcommittee responsible for conducting the annual risk assessment.
- Assess the impact of emerging regulations, technologies, and care models on the compliance program.
- Evaluate the organization's compliance program and risk assessment process against the OIG, DOJ, and COSO guidance.
- Develop a comprehensive risk assessment policy and procedure documenting the methodology.
- Identify a cyber security and compliance expert to serve on the Compliance Committee and Board.
- Conduct a thorough review of third-party vendor and partner risks.

WEBINAR OUTLINE

Introduction and Overview of Government Shutdown and Its Impact on Healthcare

- PYA Moderator introduces the webinar, mentioning the topics of focusing on compliance, risk assessments, and building blocks for annual plans.
- Speakers Shannon Sumner and Rhonda Buchholz introduce themselves and provide information about their roles and expertise.

- Shannon Sumner begins the presentation, emphasizing the importance of compliance in delivering safe and ethical healthcare.

Building Foundational Blocks for Successful Risk Assessments

- Rhonda Buckholtz discusses the importance of leadership commitment to compliance, including appointing dedicated compliance officers.
- The need for a culture of compliance is highlighted, with a focus on embedding ethical decision-making and regulatory awareness.
- Open communication and reporting mechanisms are essential for raising compliance concerns without fear of retaliation.
- Regular training and education programs are necessary to reinforce the importance of compliance and ensure employees understand the "why" behind the policies.

Identifying and Prioritizing Risks for 2026 Compliance Work Plan

- Rhonda Buckholtz explains the importance of risk assessments in identifying areas of non-compliance and prioritizing compliance activities.
- External factors such as evolving regulations and internal factors like workflows and inefficiencies should be considered in risk assessments.
- The findings from risk assessments help guide the prioritization of compliance activities, with high-risk areas receiving more attention.
- Policies and procedures should be well-thought-out and aligned with regulatory requirements, making them actionable for employees.

Training and Education in Compliance Programs

- Rhonda Buckholtz emphasizes the critical role of training in compliance programs, advocating for continuous training rather than one-time sessions.
- Orientation sessions for new hires and annual refresher courses tailored to roles are recommended.
- Scenario-based training allows employees to practice identifying and responding to compliance risks.
- Documenting training attendance and materials is essential for auditing purposes.

Auditing and Monitoring Compliance Programs

- Rhonda Buckholtz discusses the importance of auditing and monitoring to ensure policies and procedures are followed.
- Audits can take various forms, including random reviews of medical records and billing claims, and automated tools for flagging unusual billing patterns.
- Findings from audits should feed into corrective action plans, with swift action taken to correct issues and update policies if needed.
- Continuous improvement is crucial for strengthening the overall compliance framework.

Reporting and Corrective Actions in Compliance Programs

- Rhonda Buckholtz highlights the importance of clear documentation of corrective actions to demonstrate commitment to compliance.

- Employees should know how to report concerns, who will review them, and how follow-up will occur.
- Corrective actions may include revising policies, providing additional training, and self-reporting to regulatory agencies.
- Ensuring fair enforcement of policies is essential, with documentation justifying decisions and actions.

Sustaining Compliance Programs Over Time

- Shannon Sumner stresses that building a compliance program is an ongoing process, not a one-time project, and is applicable to healthcare organizations of all sizes.
- Changes in healthcare laws, technologies, and business operations require regular updates to compliance programs.
- Ongoing communication with staff and external partners helps ensure compliance remains a living, breathing part of the organization.
- Regular performance program evaluations, conducted internally or by third-party experts, identify gaps and opportunities for enhancement.
- She discusses the OIG's *Compliance Program Guidance*, the DOJ's *Evaluation of Corporate Compliance Programs*, and COSO's *Enterprise Risk Management Framework* as valuable resources.

Purpose of Risk Identification and Prioritization

- Shannon Sumner explains the purpose of conducting risk identification and prioritization, starting with understanding the risk universe.
- The importance of aligning compliance focus with the organization's strategic and operational goals is emphasized.
- Prioritization helps organizations address high-risk areas with limited resources, elevating areas that cannot be included due to resource constraints.
- Understanding the entity's risk appetite and involving key stakeholders in the risk assessment process are crucial.

Internal and External Risk Identification

- Shannon Sumner discusses identifying internal risks, such as data analysis, mergers and acquisitions, and third-party relationships.
- The importance of understanding the risk universe, including legal entities, joint ventures, and significant contracts with third parties, is highlighted.
- External risks include regulatory changes, enforcement actions, and industry benchmarking.
- Emerging technologies like AI and the Internet of Things should also be factored into the risk inventory.

Developing a Risk Inventory and Scoring Methodology

- Shannon Sumner recommends creating a formal risk inventory or registry, listing each risk with its description, regulatory reference, and source.
- Assigning a department owner or risk owner for each risk and documenting the current status and goals for mitigation and monitoring is essential.
- A simple risk scoring matrix can help prioritize risks based on likelihood, impact, regulatory scrutiny, and organizational readiness.

- Examples of high-risk areas, such as HIPAA access log violations, are provided to illustrate the scoring process.

Involving Key Stakeholders in Risk Assessment

- Shannon Sumner emphasizes the importance of involving key stakeholders, including clinical leadership, revenue cycle teams, human resources, IT and security, legal counsel, and executive leadership.
- The OIG guidance requires the Compliance Committee to coordinate with compliance audit, quality, and risk management functions for joint risk assessments.
- Continuous documentation and monitoring of risk events and adverse events through root cause analysis are crucial.
- Resources for risk assessment, such as industry publications, compliance webinars, and peer benchmarking, should be leveraged.

Risks to Consider for the 2026 Compliance Work Plan

- Shannon Sumner outlines key risks to consider for the 2026 compliance work plan, including cybersecurity threats, data privacy, and the impacts of OBA.
- The importance of having compliance and cybersecurity experts on the board is highlighted.
- Emerging technologies, quality of care, and the 340B program integrity are identified as critical areas for compliance efforts.
- The need for routine audits to preserve the 340B program and ensure compliance with regulatory requirements is emphasized.

Conclusion and Final Thoughts

- Shannon Sumner concludes the webinar by summarizing the key points and emphasizing the importance of staying informed and proactive in compliance efforts, and aware of regulatory changes.
- Rhonda Buchholz reiterates the importance of continuous monitoring and updating of risk assessments.
- The presenters and PYA Moderator conclude the webinar by thanking the audience and with information on how to access the slides, recording, and additional resources.