How to Conduct a Risk Assessment & Create A Work Plan

Presented by

SKYDA CONSULTING

Marcie Swenson, RN JD LLM CHC
Healthicity | VP Compliance & Senior Counsel

Disclaimer: Nothing in this presentation should be construed as legal advice nor relied upon as legal expertise.

What We're Going to Cover

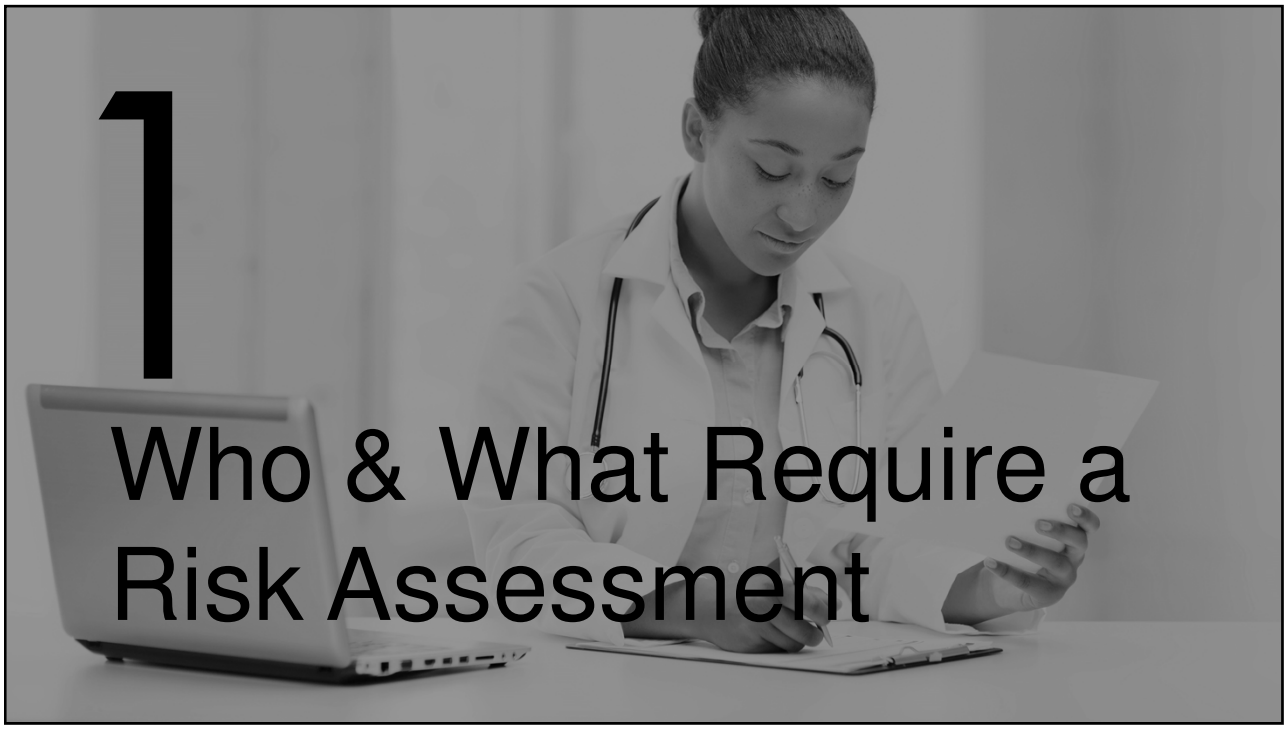
SKYDA CONSULTING

1 Who & What Require a Risk Assessment

2 Qualities of Good Risk Assessments

3 Risk Assessment Essential Steps

4 Mitigation or Work Plan



1 Who & What Require a Risk Assessment

Are Risk Assessments Required?

- U.S. Sentencing Commission Guidelines were amended to require organizations to:

  "…periodically assess the risk of criminal conduct and take appropriate steps to design, implement, or modify each requirement set forth … to reduce the risk of criminal conduct identified through this process."

- Commentary associated with these U.S. Sentencing Commission Guidelines establish qualities of a risk assessment:

  Risk nature and seriousness, likelihood, prior history, and prioritization that directs mitigation efforts to the highest risks.

Are Risk Assessments Required?

- U.S. Attorneys' Manual discusses prosecutorial considerations.
- DOJ: *Evaluation for Corporate Compliance Programs*

  "what methodology has the company used to identify, analyze, and address the particular risks it faced?"

Are Risk Assessments Required?

OIG Supplemental Compliance Program Guidance for Hospitals:

> "Has the hospital developed a risk assessment tool, which is re-evaluated on a regular basis, to assess and identify weaknesses and risks in operations; and does the risk assessment tool include an evaluation of Federal health care program requirements, as well as other publications, such as the OIG's CPGs, work plans, special advisory bulletins, and special fraud alerts?"

Are Risk Assessments Required?

- HIPAA
- HITECH
- EPA
- OSHA
- Many State Medicaid Programs

2 Qualities of Good Risk Assessments

Definition: Risk Assessment

Collecting, assessing, and evaluating the broad spectrum of risks and relevant information; conducted by multiple individuals with different functions throughout the organization; to effectively understand the aggregate relationships and implications of the information identified; and gain a perspective adequate to assess relevant risks, understand inter-relationships of risk indicators, and determine risk mitigation and control activities.

Risk Assessment Description

The compliance risk assessment will help the organization understand the full range of its risk exposure, including the likelihood that a risk event may occur, the reasons it may occur, and the potential severity of its impact. An effectively designed compliance risk assessment also helps organizations prioritize risks, map these risks to the applicable risk owners, and effectively allocate resources to risk mitigation.

- Deloitte: Compliance Risk Assessments

https://www2.deloitte.com/us/en/pages/risk/articles/compliance-risk-assessments-the-third-ingredient-in-a-world-class-ethics-and-compliance-program.html

Risk Assessment Objective

- Summarize the risk profile of the organization;
- Identify gaps and opportunities for improvement;
- Set the compliance and ethics strategy for a specified period of time (1-5 years);
- Shape the direction of the compliance program and related operations;
- Record how the assessment was conducted; and
- Used to create Annual Work Plan or mitigation plan for addressing specific risks.

The Best Compliance Risk Assessments. . .

- Gather input from a cross-functional team
- Build on what has already been done
- Establish clear risk ownership of specific risks and drive toward better transparency
- Make the assessment actionable
- Solicit external input when appropriate

The Best Compliance Risk Assessments. . .

- Treat the assessment as a living, breathing document
- Use plain language that speaks to a general business audience
- Are periodically repeated (annually)
- Leverage data

3 Risk Assessment Essential Steps

Risk Assessment Essential Steps

SKYDA CONSULTING

1. Identify Risk Assessment Director
2. Create Risk Assessment Workgroup
3. Develop risk assessment framework
4. Develop risk assessment methodology
5. Design data repository, tool, or format

Risk Assessment Essential Steps

6 Identify & involve individuals with key knowledge

7 Utilize existing data, audits, surveys, validations, etc.

8 Design an implementation plan & timeline

9 Conduct the Risk Assessment & carryout the assessment methodology

10 Prioritize risks & complete final report

Identify a Risk Assessment Director

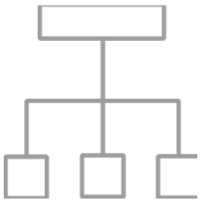
- Determine who you want to be the risk assessment director
- Help the leader understand their risk assessment assignment
- Give them the accountability and authority needed to lead the RA efforts
- Allow them to delegate assignments and responsibilities.

Create a Risk Assessment Workgroup

- Form a workgroup to help guide risk assessment activities
- Consider including individuals from different disciplines
- Include individuals that might not cooperate otherwise
- Include individuals that have taken an interest in compliance activities
- Involve individuals with influence and leadership capability

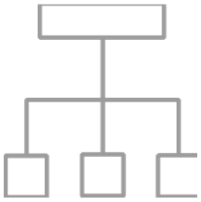
Develop a Framework

- Complex & robust risk assessments require a solid framework & methodology.
- The framework lays out the organization's compliance risk landscape and organizes it into risk domains.
- The framework needs to be comprehensive, dynamic, and customizable, allowing the organization to identify and assess all applicable categories of compliance risk.

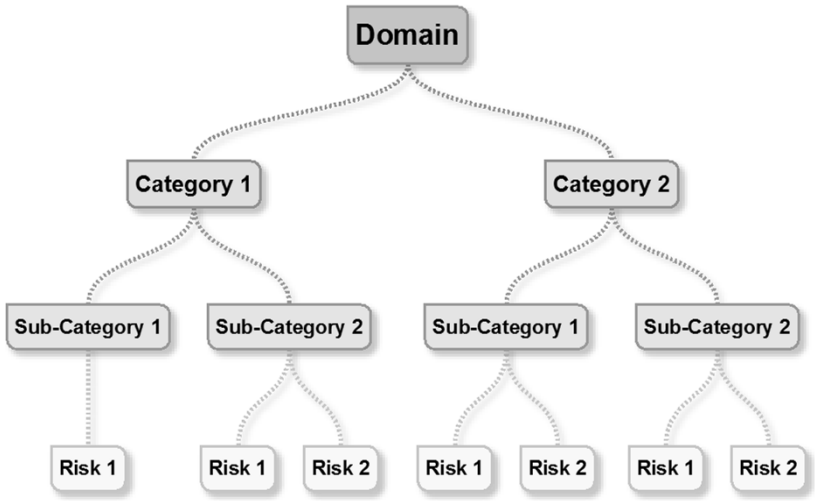


Develop a Framework

- Compliance risks can be specific to an industry; other compliance risks transcend industries or geographies.
- An effective framework should assist in an effective risk mitigation strategy (Work Plan) for priority compliance risk domains.



Framework



Scope & Categories

- Should all operations be included?
- Limit the scope to significant operations?
- Initial risk assessments should be limited in scope.
- Subsequent risk assessments can be broader due to the base findings established with prior risk assessments.

Scope & Categories

- Don't try to inventory/assess every conceivable compliance risk.
- Carve out areas that have strong ongoing auditing/monitoring.
- Realize risk assessment findings often trigger deeper assessment and audits.

Develop a Methodology

- Complex & robust risk assessments require a solid framework & methodology.
- The methodology contemplates objective & subjective ways to assess risks.
- How will the information be collected? Interviews? Surveys? Assignments?
- How will the information be organized once it is collected?

Develop a Methodology

- What type of tool or document will be used as the repository for the risk assessment data?
- How will you assess risks in a manner that allows equal comparison between risk categories and domains?
- Will you incorporate a grading or scoring methodology to assist risk prioritization?

Design a Data Repository

- How will you store and organize collected data?
- Does the tool allow comparison of data?
- Incorporate your qualitative methodology
- Incorporate ranking or scoring criteria
- Spreadsheet?
- Software?

Method?

Quantitative Method
- Numeric value: Loss Value x Probability = Risk

Qualitative Method
- Most used method & easy to prioritize risks

Qualitative Method Steps:
- Determine the likelihood of occurrence and severity of each risk
  - **Likelihood of occurrence** (remote, possible, or probable): based on findings from document review, interviews, surveys, regulation changes, education, etc.
  - **Severity** (moderate, serious, or severe): Consider the impact. Would it threaten licensure or cause loss of federal funds?
- Prioritize risks with a chart
  - Create a graph and chart/rank each risk (i.e. low, medium, high, or critical). Those risks identified as high and critical will demand the most immediate attention.

Utilize Existing Data

- **Review Internal Documents**: audits, survey findings, monitoring, internal compliance/violation trends, past risks & risk assessments, problem areas that haven't been addressed.
- **Review Available Data**: metrics and measures
- **Review Training & Education**: Is education consistent with current laws? Proper Documentation? Frequency? Addresses top areas of risk?

Data Examples

Revenue Cycle
- Billing claims denials by department
- % of total revenue by dept.
- Coding accuracy statistics and trends

Surveys
- Employee or Physician surveys
- Conflict of Interest Surveys

Events Metrics
- Compliance hotline calls
- Privacy reports vs. privacy breaches
- Patient/employee safety
- Opioid Diversion
- Nondiscrimination grievances

Physician Financial Relationships
- Physician Contract Monitoring
- Physician lease agreement/space

External Agency Surveys/Investigations
- OCR
- DOJ
- FDA

Technology
- Bio-medical equipment (FDA, recalls, reporting)
- HIPAA/Cybersecurity vulnerability
- New software/hardware risks

Identify & Involve Individuals with Key Knowledge

Risk Assessment Leader:
- Who is leading the risk assessment implementation? Compliance Officer/Director, Risk Manager, Administrator
- Authority, involved in every step, respected, and supported by leaders & employees

Risk Assessment Committee:
- Approve plan, approve assessment tool, determine categories, review assessment responses and approve risk profile, etc.
- Key knowledge experts or retained experts (i.e. data security)

Who will complete individual assessments?
- Administration
- Program or Department Managers
- Employees
- Patients

Design an Implementation Plan & Timeline

- How will the risk assessment be completed?
- What is the timeline or target completion date?
- Set small achievable steps and deadlines
- Allow 30-60 days to conduct the risk assessment
- Divide the risk assessment into manageable segments (similar risk areas or method of information gathering)
- Focusing on segments allows method testing and modifications as the risk assessment progresses

Conduct the Risk Assessment

- Conduct interviews, questionnaires, surveys, open discussion forums, etc.
- Gather existing data and blend it with from interviews, questionnaires, and surveys
- Distribute and collect written assessments (digital, email, or spreadsheet)
- Compile in the risk assessment tool/repository

Interview Examples

Manager Interview:

1. What is your perception of how well we comply with federal, state, and local laws and regulations?
2. What do you think are the major operational risks?
3. Are there proper methods in place to ensure that appropriate corrective actions are taken when audits reveal deficiencies?
4. Is there anything that keeps you up at night?

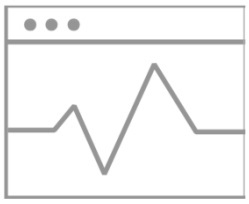
Interview Examples

Employee Interview:

1. Are there certain risks that often go overlooked?
2. What risks are less likely to happen but might have a major impact on the hospital if they occur?
3. Is there any inefficiency (financial, managerial, or other) in your functional area? Are there ways to prevent these?
4. Would you say that our hospital has a positive "culture of compliance?" Why or why not?
5. How are you trained on compliance?
6. How are new regulations or policies identified and distributed?
7. Are you and your colleagues quick to comply with new hospital policies, or is there a tendency to continue to function under old practices and to refuse to adapt?

Prioritize Risks

- Compare risks across domains and categories
- Prioritize risks by individual risk or by category
- Step back; does the ranking make sense?
- What risks will you try to mitigate?



Risk Profile/Ranking

Impact Severity				
	Severe	Medium	High	Critical
	Serious	Low	Medium	High
	Moderate	Low	Low	Medium
		Remote	**Possible**	**Probable**
		Likelihood of Occurrence		

Complete Final Risk Report

- Include information about the importance of conducting a risk assessment
- Set the compliance and ethics strategy for a specified period of time (1-5 years);
- Shape the direction of the compliance program and related operations;
- Used to create Annual Work Plan or action plan for addressing specific risks.

Complete Final Risk Report

Create a final report that explains:

- Risk assessment process
- Framework
- Methodology
- Data Sources
- Participants
- Opportunities for Improvement
- Highlights Highest Risks

Risk Assessment vs. Work Plan

Risk Assessment: Determines Risk

- Collects data
- Determines total compliance risk
- Prioritizes or ranks risk

Work Plan: Action to Mitigate Risk

- Facilitates risk mitigation
- Assigns accountability to specific individuals
- Establishes an action plan (audits, monitoring, policies, education)
- Establishes deadlines
- Provides a record of corrective action

Audit Plan vs. Work Plan?

- Determining scope or severity of risk? (Audit/Assessment)
- Are you mitigating risk? (Work)
- Are you examining current controls? (Audit/Assessment)
- Are you implementing new controls? (Work)
- Corrective Action? (Work)

Work Plan Components

- Domain, category, sub-category, risks
- Scope, laws, & regs
- Accountable person
- Division, department, or service line
- Goals
- Action/mitigation plan & deadlines
- Current controls/needed controls
- Testing & monitoring (existing and needed)
- Status indicators
- Status notes

Accountable Person & Department/Service Line

- Expert
- Department Manager
- Already working on related projects
- Responsible for monitoring activities related to the goal
- Consider burden on the individual
- Identify department/service line most related to the goal
- More than 1 individual can be accountable

Goal

Definable Goal:

Educate ED workforce on EMTALA form completion by 10/15/18; by 12/15/18 EMTALA forms monitoring will demonstrate 100% accuracy.

- S – Specific
- M – Measurable
- A – Attainable*
- R – Relevant
- T – Time-Based

*Attainable actions may not result in total mitigation of risk.

Corrective Action, Mitigation & Deadlines

- Main purpose is to eliminate/mitigate risk and achieve the goal
- Determine specific steps necessary to accomplish the goal
- Analyze each step to ensure it supports the goal
- Establish a time line & deadline for each action step
- Be realistic – sometimes risk cannot be eliminated
- Occasionally there are no actions or additional controls that can be carried out to reduce risk. (i.e. Ransomware/Malware)
- Ensure all controls have been considered

Mitigation Controls

- Compare current controls vs. needed controls
- Policies, procedures, guidelines, charters, code of conduct (including distribution and education)
- Committees & work groups
- Monitoring & understanding new laws, regulations, rules
- Education associated with new laws, regulations, rules
- Sufficient staff and funding to support compliance initiatives & completion of work plan
- Compliance specific education (physicians, vendors, contractors)

Monitoring/Testing

The most effective means to determine whether a compliance plan is successful is to monitor activities in relation to applicable laws and regulations.

- Design a monitoring tool or test
- Random sampling
- Interviews
- Survey
- Observing behavior or activity in question
- Modify work plan according to findings

Status Indicators, Updates & Notes

- Update goals and actions frequently
- Proper oversight requires status SU to determine:
  - If actions are working; or
  - If something needs to be changed
- SUs: keep the target in sight and creates accountability
- Use visual status indicators: gold stars, green, red, yellow
- Status notes: relevant to each action for each work plan risk/goal
- Explanation of why actions were not taken or achieved (when needed)

Questions?

MarcieS@MySkyda.com
Marcie.Swenson@Healthicity.com

Disclaimer: Nothing in this presentation should be construed as legal advice nor relied upon as legal expertise.