

Accurately Assess Your Risk Landscape:

How to Design a Risk Assessment Framework & Methodology



Presented by

Marcie Swenson, RN JD LLM CHC
Skyda Consulting & Law Group



SKYDA

DISCLAIMER REGARDING LEGAL ADVICE: None of the information contained in this document is intended to constitute legal or other professional advice, and you should not rely solely on the information contained herein for making legal decisions. When necessary, you should consult with an attorney for specific advice tailored to your situation.

- Fraud, Waste, & Abuse
- Government Relations
- Policy, Code of Ethics
- MD, RNs, Pharmacist
- Biomedical Engineer
- Lab, Pharmacy, Imaging
- Physician Contracting
- Lease Agreements
- Clinical Serv. Contracts
- Reimbursement

- Certified Coders
- Medicare/Medicaid
- Privacy/Security/HIM
- Medical Staff

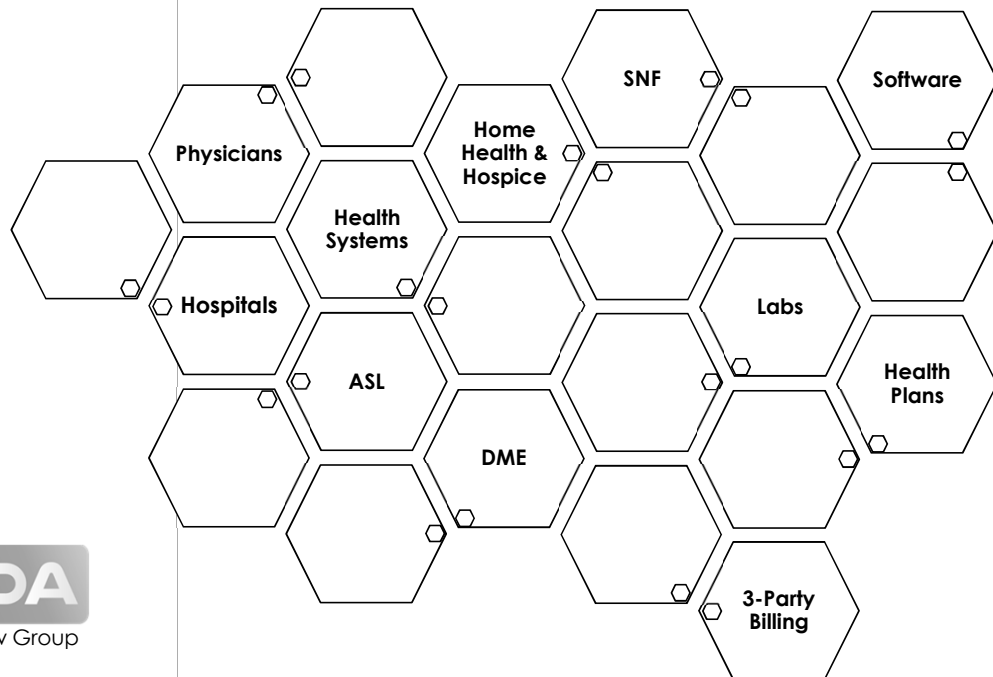
- Medical Documentation
- Municipality Compliance
- Procurement Contracts
- Compliance Officers
- HR, OSHA, EOC
- Program Effectiveness
- Program Workflow
- Risk Assessments
- Mitigation Strategy
- Regulation Interpretation

Attorneys, Consultants, & Advisors



SKYDA

Our Clients



SKYDA
Consulting & Law Group



What We're Going to Cover

1. Is a Risk Assessment Required?
2. Qualities of Good Risk Assessments
3. Essential Steps
4. Framework & Scope
5. Methodologies
6. Risk Assessment Report



1



Is a Risk Assessment Required?



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.”
- U.S. Sentencing Commission Guidelines Commentary establish qualities of a risk assessment:
 - Risk nature and seriousness, likelihood, prior history, and prioritization that directs mitigation efforts to the highest risks.

SKYDA

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?”

SKYDA

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?”

SKYDA

Are Risk Assessments Required?

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

SKYDA

Consulting & Law Group

2

Qualities of Good Risk Assessments

SKYDA

Consulting & Law Group

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.

SKYDA

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>

SKYDA

Risk Assessment Objective

The final product of a compliance risk assessment should:

- 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 action plan for addressing specific risks.

SKYDA

HCCA Seven Component Framework for Auditing/Monitoring

CH3
MS10

- Perform a risk assessment and determine the level of risk
- Understand laws and regulations
- Obtain and/or establish policies for specific issues and areas
- Educate on the policies and procedures, and communicate awareness
- Monitor compliance with laws, regulations, and policies
- Audit the highest risk areas
- Re-educate staff on regulations and issues identified in the audit

SKYDA

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

SKYDA

Slide 15

CH3 should this be Auditing and Monitoring, as I know you're not a fan of using the two synonymously?

Cory Hammond, 5/15/2018

MS10 Yes, It's ok because HCCA uses them together. I don't mind auditing and monitoring together. I just like to keep risk assessment and work plan separate and auditing/monitoring separate from risk assessment. OK did that confuse you enough.
lol

Marcie Swenson, 5/15/2018



The Best Compliance Risk Assessments

- Treat the assessment as a living, breathing document
- Use plain language that speaks to a general business audience
- Periodically repeat the risk assessment
- Leverage data

SKYDA



Compliance Risk Assessment vs. Other Risk Assessments

Compliance

Compliance with federal, state, and local laws, regulations, and rules.

Operational

Possibility of loss to buildings, office equipment, personal property, vehicles, and other physical assets.

Financial

Addresses concerns related to solvency, grants management issues, submission of accurate claims, appropriate documentation, sound procurement practices, appropriate fiscal management standards and cash drawdown policies, reserves, and investments.

SKYDA



Compliance Risk Assessment vs. Other Risk Assessments



Clinical


Medical Staffing credentialing, medical malpractice, patient safety, informed consent, medication administration, experimental procedures, clinical research, and medical records.

Legal

Risk of being sued: tort liability for non-clinical injuries, breach of contract, prohibited conduct of practices, medical malpractice, breach of fiduciary duties, FCA, discrimination and wrongful termination.

SKYDA

3



Risk Assessment Essential Steps

SKYDA

Consulting & Law Group



Risk Assessment Essential Steps

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

SKYDA



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 chosen assessment methodologies
10. Prioritize risks & complete final report

SKYDA



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.

SKYDA

MS11



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

SKYDA

Slide 24

MS11 Can the third bullet be changed to "might not otherwise cooperate?"

Marcie Swenson, 5/15/2018

4

Risk Assessment Framework & Scope

SKYDA

Consulting & Law Group

Develop a Framework

- Complex & robust risk assessments require a solid framework.
- 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.

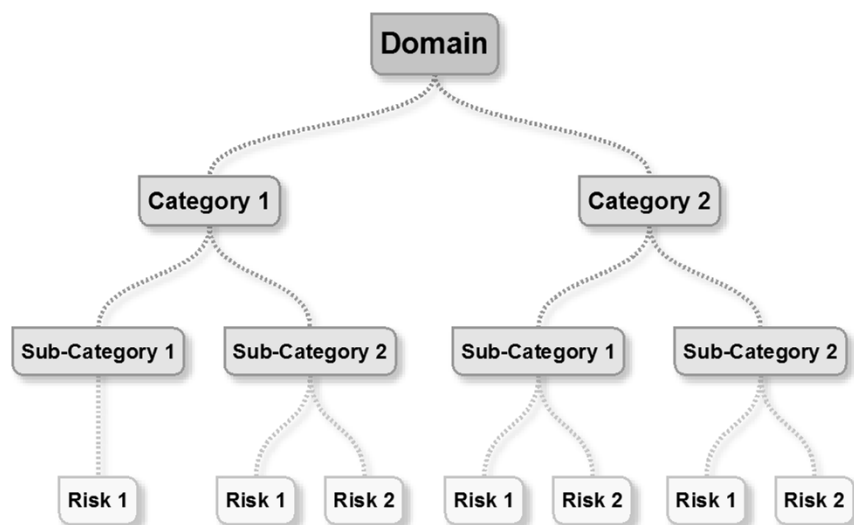
SKYDA

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.

SKYDA

Framework



SKYDA



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.





Get Started On Your Framework

- Big Auditing Firms has some examples – such as Deloitte, Ernest & Young, etc.
- Online examples used by various organizations
- HCCA Compliance Weekly News & *Compliance Today*
- *Compliance Insight* – Newsletter
MySkyda.com



5

Risk Assessment Methodologies



Develop a Methodology

- Complex & robust risk assessments require a solid 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, Tool, or Format

- 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: $\text{Loss Value} \times \text{Probability} = \text{Risk}$

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?
- Construct a risk profile
 - 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?

SKYDA

Data Examples

Revenue Cycle

- Billing/claims denials by department
- Coding accuracy statistics and trends

Surveys

- Employee or Physician surveys
- Conflict of Interest Surveys

Technology

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

- Compliance hotline calls
- Privacy reports vs. privacy breaches
- Patient/employee safety
- Opioid diversion
- Discrimination grievances

Physician Financial Relationships

- Physician contract monitoring
- Physician lease agreement

External Agency Surveys & Investigations

- OCR, DOJ, FDA, OSHA, TJC

SKYDA

Identify & Involve Individuals with Key Knowledge

Risk Assessment Leader:

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

- Key knowledge experts or retained experts (i.e. data security)

Who will complete individual assessments?

- Administration
- Program or Department Managers
- Employees
- Patients

Risk Assessment Committee:

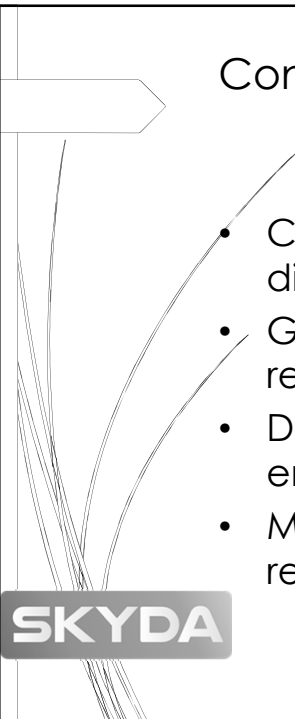
- Approve plan, approve assessment tool, determine categories, review assessment responses and approve risk profile, etc.

SKYDA

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).
- Start with small segments this allows method testing and modifications as the risk assessment progresses.

SKYDA



Conduct the Risk Assessment & Carryout the Assessment Methodology

- Conduct interviews, questionnaires, surveys, open discussion forums, etc.
- Gather existing data and blend it with interview results, questionnaires, and survey information.
- Distribute and collect written assessments (digital, email, or spreadsheet).
- Migrate all data into the risk assessment tool, repository, or document.

SKYDA



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 health center deficiencies?
4. Is there anything that keeps you up at night?

SKYDA



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 "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?

SKYDA

6



Risk Assessment Report

SKYDA

Consulting & Law Group

First 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; and
- Use to create Annual Mitigation/Work Plan or action plan to minimize high risks.

SKYDA

Complete Final Risk Report

- Explain risk assessment process
- Display risk assessment framework
- Describe risk assessment methodology
- Include data sources & participants
- Identify opportunities for Improvement
- Highlight highest risks

SKYDA
Consulting & Law Group



Risk Assessment vs. Work Plan

Risk Assessment: Determines Risk

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

Work Plan: Action Plan 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

SKYDA



Final Suggestion:

Dive in now and get your first risk assessment experience!

Don't delay; start next week; it's ok if the first risk assessment isn't perfect.

SKYDA



Questions?

Marcie Swenson, RN JD LLM CHC

MarcieS@MySkyda.com 1.866.My.Skyda MySkyda.com

DISCLAIMER REGARDING LEGAL ADVICE: None of the information contained in this document is intended to constitute legal or other professional advice, and you should not rely solely on the information contained herein for making legal decisions. When necessary, you should consult with an attorney for specific advice tailored to your situation.