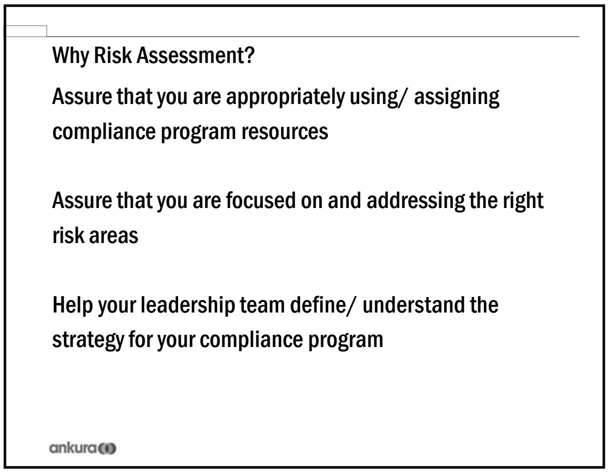
Data Driven
Compliance Risk Assessment

Steven W. Ortquist, CHC-F
Senior Managing Director, Ankura

ankura

ankura.com



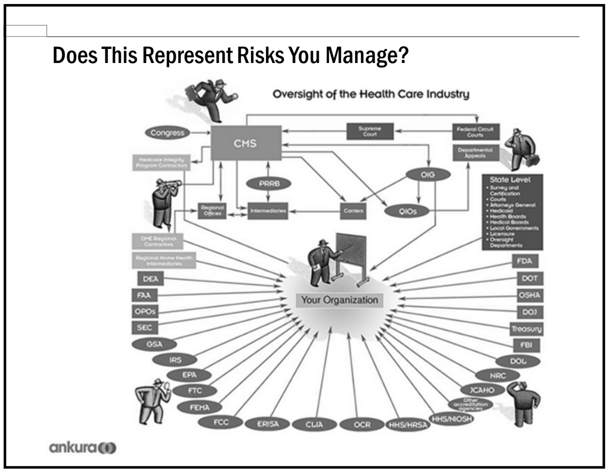
Why Risk Assessment?

Assure that you are appropriately using/ assigning compliance program resources

Assure that you are focused on and addressing the right risk areas

Help your leadership team define/ understand the strategy for your compliance program

ankura



Does This Represent Risks You Manage?

ankura

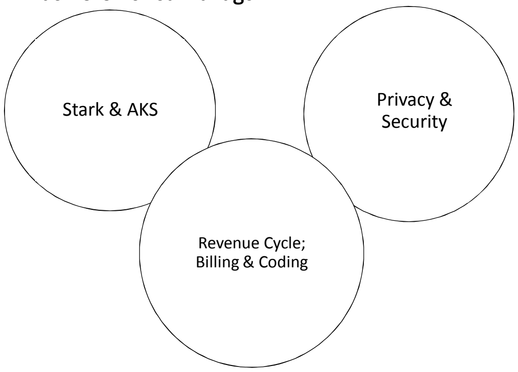
What Risks Does Your Program Manage?

What would your leadership team say?

What are the characteristics of risks they want you to help them avoid?

Do you really have compliance program resources to manage every conceivable regulatory requirement?

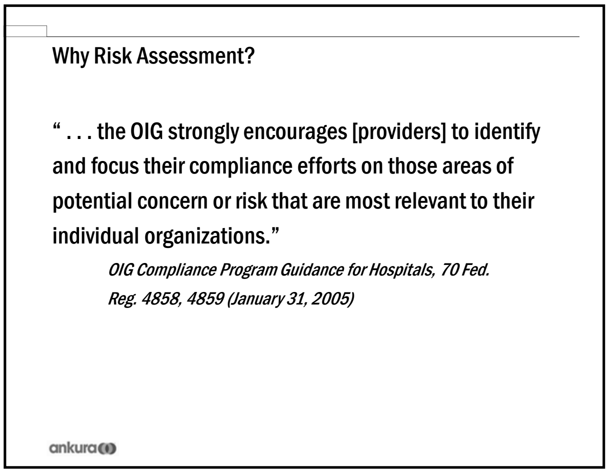
What Risks Do You Manage?



Why Risk Assessment?

"(c) In implementing [a compliance program], the organization shall periodically assess the risk of criminal conduct and shall take appropriate steps to design, implement, or modify each [compliance program element] to reduce the risk of criminal conduct identified through this process."

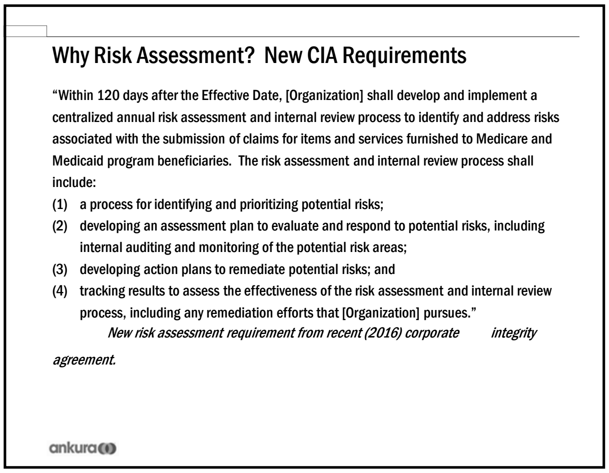
USSG §8B2.1.(c)



Why Risk Assessment?

"... the OIG strongly encourages [providers] to identify and focus their compliance efforts on those areas of potential concern or risk that are most relevant to their individual organizations."

OIG Compliance Program Guidance for Hospitals, 70 Fed. Reg. 4858, 4859 (January 31, 2005)



Why Risk Assessment? New CIA Requirements

"Within 120 days after the Effective Date, [Organization] shall develop and implement a centralized annual risk assessment and internal review process to identify and address risks associated with the submission of claims for items and services furnished to Medicare and Medicaid program beneficiaries. The risk assessment and internal review process shall include:

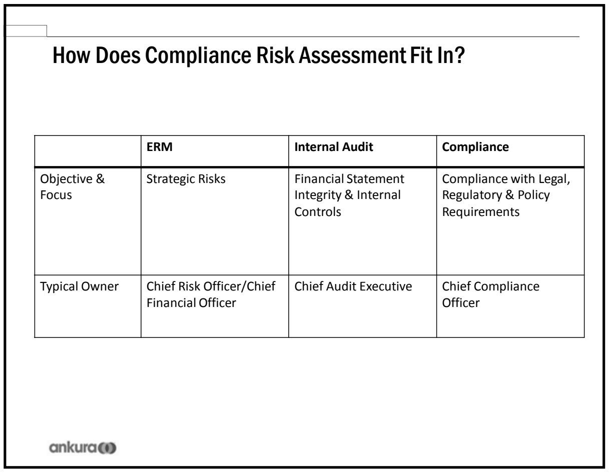
(1) a process for identifying and prioritizing potential risks;

(2) developing an assessment plan to evaluate and respond to potential risks, including internal auditing and monitoring of the potential risk areas;

(3) developing action plans to remediate potential risks; and

(4) tracking results to assess the effectiveness of the risk assessment and internal review process, including any remediation efforts that [Organization] pursues."

New risk assessment requirement from recent (2016) corporate integrity agreement.



How Does Compliance Risk Assessment Fit In?

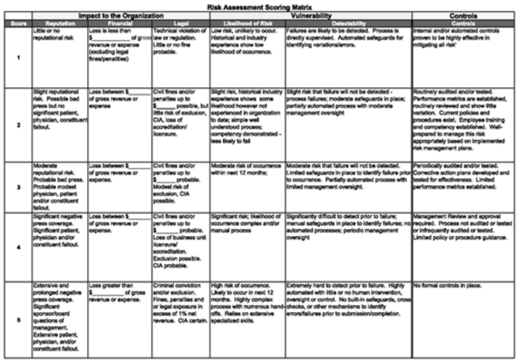
	ERM	Internal Audit	Compliance
Objective & Focus	Strategic Risks	Financial Statement Integrity & Internal Controls	Compliance with Legal, Regulatory & Policy Requirements
Typical Owner	Chief Risk Officer/Chief Financial Officer	Chief Audit Executive	Chief Compliance Officer

Typical Risk Assessment Process

- Identification of compliance risks
- Evaluation of identified risks
  - Risk Impact: (Financial, Reputational, Legal)
  - Vulnerability: (Likelihood, Detectability)
- Prioritization of risks
- Plan/develop mitigation strategies
- Re-evaluate: Do it again!

Typical Risk Assessment Process

- Identification of compliance risks
  - OIG Workplan
  - Recent Settlements
  - Organization's Recent Experience
  - Interviews/Surveys of Leadership
  - Other

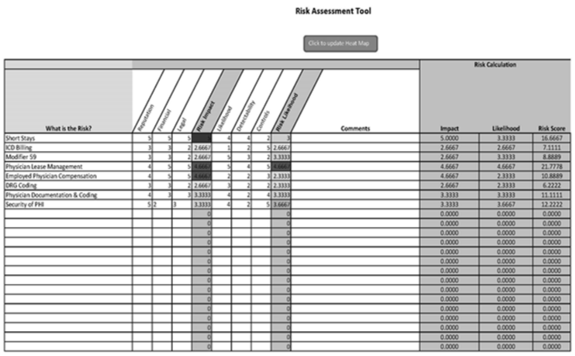


Risk Assessment Scoring Matrix

	Impact to the Organization			Vulnerability		Controls
Score	Reputation	Financial	Legal	Likelihood of Risk	Detectability	Controls
1	Little or no reputational risk	Loss is less than $____________ of gross revenue or expense (excluding legal fines/penalties)	Technical violation of law or regulation. Little or no fine probable.	Low risk, unlikely to occur. Historical and industry experience show low likelihood of occurrence.	Failures are likely to be detected. Process is directly supervised. Automated safeguards for identifying variations/errors.	Internal and/or automated controls proven to be highly effective in mitigating all risk'
2	Slight reputational risk. Possible bad press but no significant patient, physician, constituent fallout.	Loss between $_______ of gross revenue or expense	Civil fines and/or penalties up to $_______ possible, but little risk of exclusion, CIA, loss of accreditation/ licensure.	Slight risk, historical industry experience shows some likelihood however not experienced in organization to date; simple well understood process; competency demonstrated - less likely to fail	Slight risk that failure will not be detected - process failures; moderate safeguards in place; partially automated process with moderate management oversight	Routinely audited and/or tested. Performance metrics are established, routinely reviewed and show little variation. Current policies and procedures exist. Employee training and competency established. Well-prepared to manage this risk appropriately based on implemented risk management plans.
3	Moderate reputational risk. Probable bad press. Probable modest physician, patient and/or constituent fallout.	Loss between $_______ of gross revenue or expense.	Civil fines and/or penalties up to $_______ probable. Modest risk of exclusion, CIA possible.	Moderate risk of occurrence within next 12 months;	Moderate risk that failure will not be detected. Limited safeguards in place to identify failure prior to occurrence. Partially automated process with limited management oversight.	Periodically audited and/or tested. Corrective action plans developed and tested for effectiveness. Limited performance metrics established.
4	Significant negative press coverage. Significant patient, physician and/or constituent fallout.	Loss between $_______ of gross revenue or expense.	Civil fines and/or penalties up to $_______ probable. Loss of business unit licensure/ accreditation. Exclusion possible. CIA probable.	Significant risk; likelihood of occurrence complex and/or manual process	Significantly difficult to detect prior to failure; manual safeguards in place to identify failures; no automated processes; periodic management oversight	Management Review and approval required. Process not audited or tested or infrequently audited or tested. Limited policy or procedure guidance.
5	Extensive and prolonged negative press coverage. Significant sponsor/board questions of management. Extensive patient, physician, and/or constituent fallout.	Loss greater than $____________ of gross revenue or expense.	Criminal conviction and/or exclusion. Fines, penalties and or legal exposure in excess of 1% net revenue. CIA certain.	High risk of occurrence. Likely to occur in next 12 months. Highly complex process with numerous hand-offs. Relies on extensive specialized skills.	Extremely hard to detect prior to failure. Highly automated with little or no human intervention, oversight or control. No built-in safeguards, cross checks, or other mechanisms to identify errors/failures prior to submission/completion.	No formal controls in place.

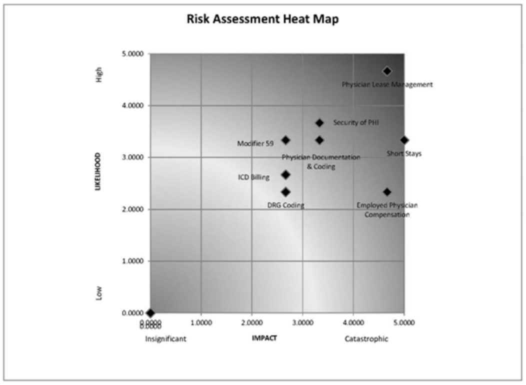
Typical Risk Assessment Process

- Impact Score
  (Financial + Reputational + Legal)
- Vulnerability Score
  (Impact Score x likelihood x detectability)
- Risk Prioritization
  - No controls – Vulnerability Score x 100%
  - Limited controls – Vulnerability Score x 75%
  - Some formal controls – Vulnerability Score x 50%
  - Adequate controls – Vulnerability Score x 25%
  - Complete controls – Vulnerability Score x 0%

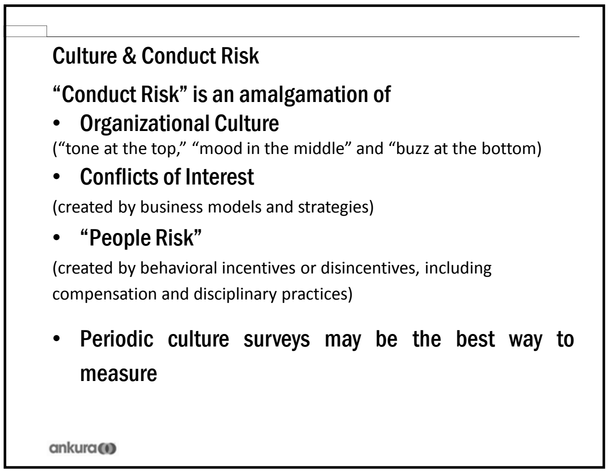


Risk Assessment Tool

										Risk Calculation		
What is the Risk?	Reputation	Financial	Legal	Risk Impact	Likelihood	Detectability	Controls	Risk Likelihood	Comments	Impact	Likelihood	Risk Score
Short Stays	5	5	5	5	4	4	2	3		5.0000	3.3333	16.6667
ICD Billing	3	3	2	2.6667	1	2	5	2.6667		2.6667	2.6667	7.1111
Modifier 59	3	3	2	2.6667	5	3	2	3.3333		2.6667	3.3333	8.8889
Physician Lease Management	4	5	5	4.6667	5	4	5	4.6667		4.6667	4.6667	21.7778
Employed Physician Compensation	4	5	5	4.6667	2	2	3	2.3333		4.6667	2.3333	10.8889
DRG Coding	3	3	2	2.6667	3	2	2	2.3333		2.6667	2.3333	6.2222
Physician Documentation & Coding	4	3	3	3.3333	4	2	4	3.3333		3.3333	3.3333	11.1111
Security of PHI	5	2	3	3.3333	4	2	5	3.6667		3.3333	3.6667	12.2222
				0				0		0.0000	0.0000	0.0000
				0				0		0.0000	0.0000	0.0000
				0				0		0.0000	0.0000	0.0000
				0				0		0.0000	0.0000	0.0000
				0				0		0.0000	0.0000	0.0000
				0				0		0.0000	0.0000	0.0000
				0				0		0.0000	0.0000	0.0000
				0				0		0.0000	0.0000	0.0000
				0				0		0.0000	0.0000	0.0000
				0				0		0.0000	0.0000	0.0000
				0				0		0.0000	0.0000	0.0000
				0				0		0.0000	0.0000	0.0000
				0				0		0.0000	0.0000	0.0000
				0				0		0.0000	0.0000	0.0000
				0				0		0.0000	0.0000	0.0000



Risk Assessment Heat Map



Culture & Conduct Risk

"Conduct Risk" is an amalgamation of

- Organizational Culture

("tone at the top," "mood in the middle" and "buzz at the bottom)

- Conflicts of Interest

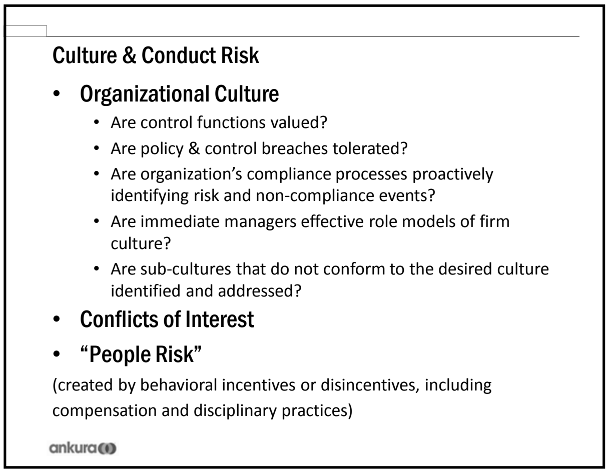
(created by business models and strategies)

- "People Risk"

(created by behavioral incentives or disincentives, including compensation and disciplinary practices)

- Periodic culture surveys may be the best way to measure

ankura

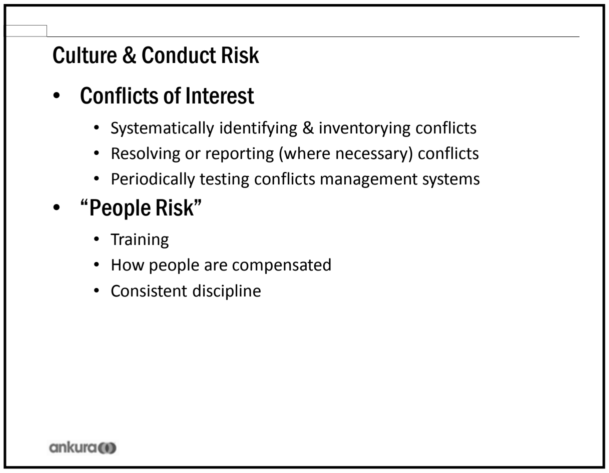


Culture & Conduct Risk

- Organizational Culture
  - Are control functions valued?
  - Are policy & control breaches tolerated?
  - Are organization's compliance processes proactively identifying risk and non-compliance events?
  - Are immediate managers effective role models of firm culture?
  - Are sub-cultures that do not conform to the desired culture identified and addressed?
- Conflicts of Interest
- "People Risk"

(created by behavioral incentives or disincentives, including compensation and disciplinary practices)

ankura



Culture & Conduct Risk

- Conflicts of Interest
  - Systematically identifying & inventorying conflicts
  - Resolving or reporting (where necessary) conflicts
  - Periodically testing conflicts management systems
- "People Risk"
  - Training
  - How people are compensated
  - Consistent discipline

ankura