Effective Risk Assessment and Audit Planning

Jim Kreiser, Principal; CRMA, CISA, CFSA

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Create Opportunities

Discussion Objectives

1. Identify factors driving the need for Risk Assessment and alignment with audit procedures

2. Discuss processes for establishing criteria over audit procedures, metrics, and reporting

3. Recognize key items and leading practices for building a robust, mature, and effective risk assessment

4. Assess methods for leveraging and incorporating risk assessments into effective and detailed audit plans

Factors Driving Risk Management:

Why Do You Do It?

What is Risk Management and Risk Assessment?

- Risk is defined as the possibility that an event will occur and adversely affect the achievement of objectives. Risk assessment involves a dynamic and iterative process for identifying and assessing risks to the achievement of objectives. Risks to the achievement of these objectives from across the entity are considered relative to established risk tolerances. Thus, risk assessment forms the basis for determining how risks will be managed.

- A precondition to risk assessment is the establishment of objectives, linked at different levels of the entity.
  - - COSO Enterprise Risk Assessment – 2013 Framework

Benefits of Risk Assessments (and/or ERM)

- Create a more risk aware culture
- Align risk appetite and strategy
- Enhance risk response decisions
- Minimize operational surprises and losses
- Identify and manage cross-enterprise risks
- Provide integrated responses to multiple risks
- Seize opportunities
- Support cost management efforts
- Improve operational performance
- Provide better basis for allocating resources

And thereby:

- Restore and/or retain stakeholder trust and confidence
- Protect and increase value for the organization and your customers
- **BETTER ALIGN AND IDENTIFY INTERNAL AUDIT ACTIVITIES**

Questions Auditors Should Ask About the RA

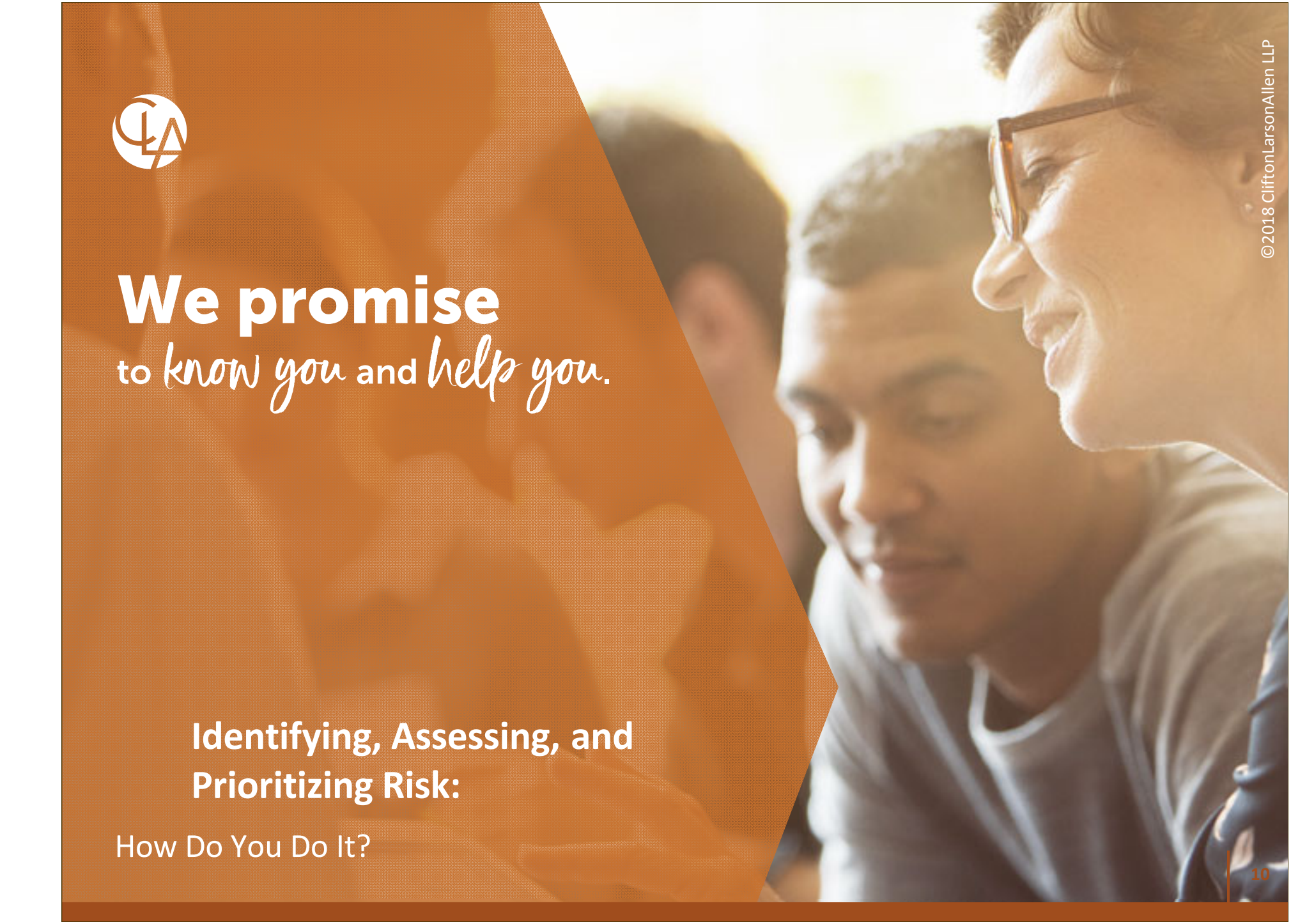
- What risks should we be focusing on? Do we know what our true top risks are?
- How well are we doing with the risks we are focusing on?
- How do we capture future risks and integrate them into the process?
- How aligned are we as an organization to make this happen?
- ***Are key risks and organizational objectives and investment aligned?? What role is audit playing? (consultative, compliance, performance, etc.)***

Governmental Risks?

- Examples of Key Risks?
  - ***Emerging Risks***
  - ***Reputational (how to assess against typical models?)***
  - ***Financial/Reporting***
  - ***Operational***
  - ***Governance***
  - ***Execution/Mission***
  - ***Grant***
  - ***Privacy/Data Risk***
  - ***Interagency***
  - ***Vendor/Third Party***

Perspective on Risk

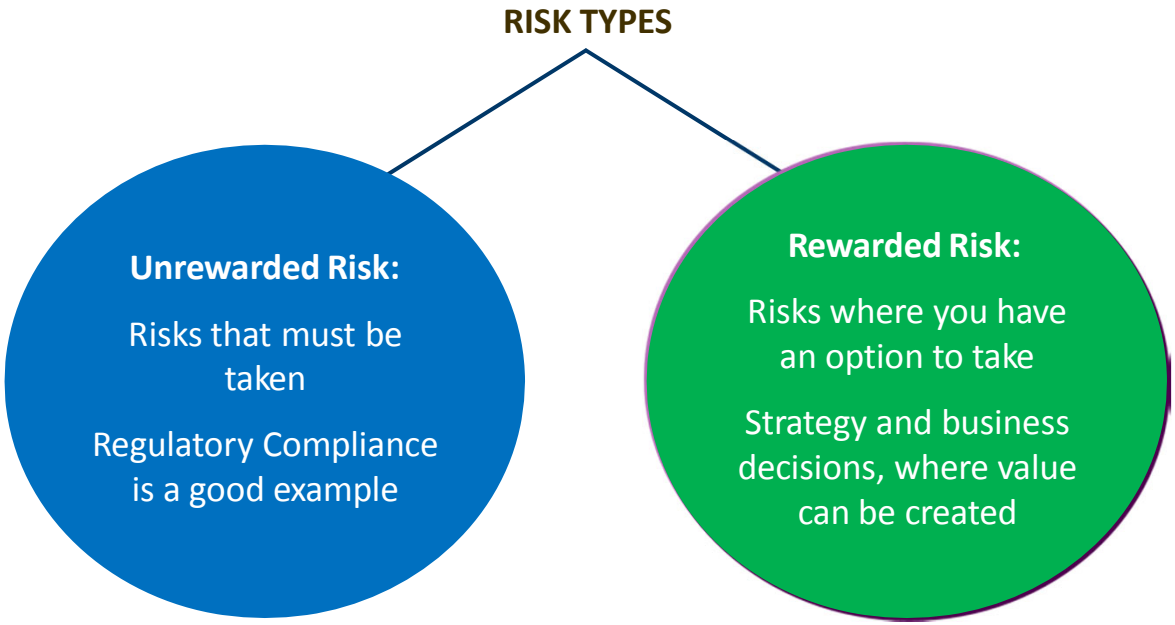
- Whether through internal audit, or organizationally, certain aspects of risk management should be defined across the entity. These parameters will help enable consistent approaches to risk assessment for audit planning.
- Risk Tolerance – acceptable level of uncertainty or variability of outcomes related to performance measures or specific objectives of the organization
- Risk Appetite – broad description of the level/amount of risk an organization is willing to take as part of its goals/strategy
- Definitions vary – so make certain your organization has a consistent definition and framework for these concepts.
- https://www.rims.org/resources/ERM/Documents/RIMS_Exploring_Risk_Appetite_Risk_Tolerance_0412.pdf



Identifying, Assessing, and Prioritizing Risk:

How Do You Do It?

The Two Sides of the Risk Coin

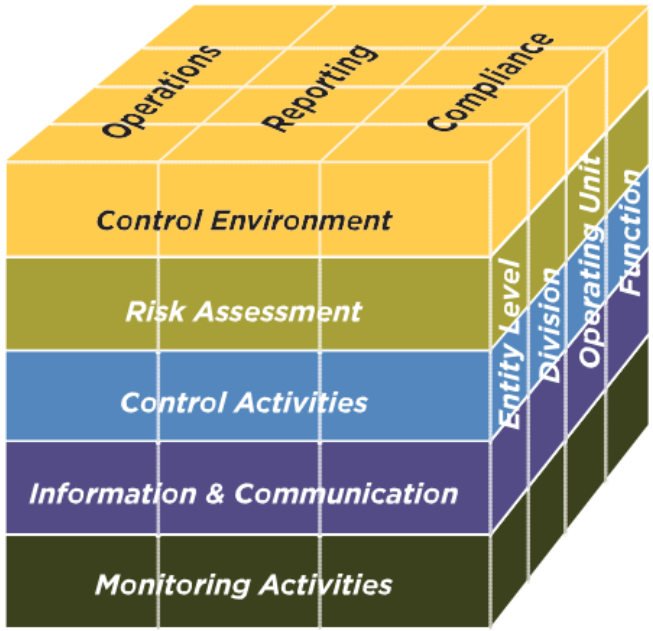


Fail to manage the Unrewarded Risks and negative implications ensue

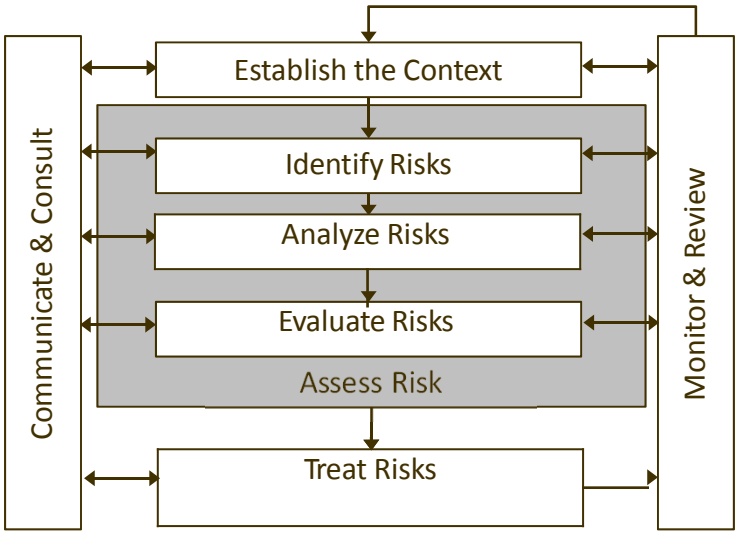
Fail to take the right amount of Rewarded Risks and you miss opportunities

Two Popular Risk Frameworks

COSO integrated framework - 2013



AS/NZ - ISO 31000:2009



Shortcomings of the COSO approach

Estimating Likelihood and Impact

"Uncertainty of potential events is evaluated from two perspectives – likelihood and impact. Likelihood represents the possibility that a given event will occur, while impact represents its effect... It is important that the analysis be rational and careful… The time horizon used to assess risks should be consistent with the time horizon of the related strategy and objectives…

For example, a company operating in California may consider the risk of an earthquake disrupting its business operations. Without a specified risk assessment time horizon, the likelihood of an earthquake exceeding 6.0 on the Richter scale is high, perhaps virtually certain. On the other hand, the likelihood of such an earthquake occurring within two years is substantially lower. By establishing a time horizon, the entity gains greater insight into the relative importance of the risk and an enhanced ability to compare multiple risks."

COSO ERM Sept 2004 p. 58

Problems With the Likelihood Model

- Little or no predictive value in context of typical planning horizons
- 80% of all major value losses are high impact / low likelihood
- Biases management to direct resources to high impact / high likelihood events at the expense of high impact / low likelihood events
- Typically focuses on single events rather than a series of events or domino effect
- Audit activities are often mis-directed to the red zone

Other models can include various assessment and classifications, including:

- Frequency to onset (has become quite common/popular)
- Pervasiveness (relative based on organization size and complexity)
- Complexity
- Etc.

Another Way to Think/Conceptualize the Risk Assessment and Planning

- Key is to utilize an approach and framework that works for the organization and can integrate with the internal audit and audit committee objectives.

- Illustrative Model:
  - Level of Control Documentation and Governance
    - Size or Volume of Transactions/Accounts
    - New Products or Systems
    - Personnel Quals and Turnover
    - Complexity
    - Susceptibility to Fraud
    - Results/Time of Last Review or Audit
    - Information and Reporting (confidential, financial, sensitive, etc.)
    - Prior Issues Reported/unresolved

  – Evaluate each item on scale, and apply weightings for each risk category across functions, units, processes, etc.

Risk Rankings?

- What is the model to utilize for ranking risks?
  - High, Medium, and Low
    - What if the risk universe/population is 200 items?
      - Standard expectation would be 20% High, 60% Medium, and 20% Low
        - That could mean as many as 40 high risk items
          - Can audit or RM effectively monitor/assess 40 risks?
  - Numeric Quantification
    - Apply ratings of 1-5 for each risk category
    - Numeric calculated values for each risk
    - Helps to delineate and refine the listing
    - See example on next page

Risk Assessment Example

		15%	10%	10%	15%	10%	10%	10%	10%	10%	100%
	Risk	Level of documented control procedures	Size or volume	New products, services, or processing systems	Personnel turnover and mix	Complexity	Susceptibility to fraud	Information and reporting	Length of time since the area was reviewed	Volume and severity of issues previously identified	Total Score
1	Data Protection	2.00	4.00	5.00	4.00	5.00	2.00	3.00	3.00	5.00	3.11
2	Network/Perimeter Monitoring	2.00	4.00	5.00	4.00	4.00	4.00	4.00	1.00	4.00	3.10
3	Vendor Management	2.00	3.00	4.00	4.00	4.00	2.00	3.00	3.00	1.00	2.80
4	Capital Commitments - Construction (CIP)/Fixed Assets	2.00	4.00	4.00	2.00	3.00	2.00	4.00	2.00	1.00	2.50
5	Pricing Pressures - Managed Care, Governmental, Pharmaceutical, Quality-Based Reimbursement, and payor risk	2.00	4.00	1.00	1.00	5.00	1.00	4.00	5.00	1.00	2.45
6	Competition - ACO, Population Management, Acute Care Hospitals, Physician-Owned Specialty Hospitals, Outpatient Facilities, Tiering/Certification	2.00	4.00	4.00	1.00	3.00	1.00	3.00	5.00	1.00	2.45
7	Labor Relations/ Union	1.00	4.00	1.00	4.00	3.00	1.00	3.00	5.00	1.00	2.45
8	Recruiting/Retention/Succession Planning -Competitive Salary and Staffing Risk for Surgical and Key Medical Staff	2.00	4.00	1.00	4.00	3.00	1.00	3.00	2.00	1.00	2.30

Risk Assessment Example – Risk Universe (ERM)

Audit Universe

The scope of enterprise-wide risk assessment included the following functional areas and processes within the Organization:

- Accounts Payable Management
- Accounts Receivable Management
- Anti-Trust/Competitive Practices
- Bad Debt & Managed Care Reserves
- Board Performance/Oversight Responsibilities
- Budgeting & Forecasting
- Cafeteria
- Capital Commitments – Construction (CIP)/Fixed Assets
- Cash Disbursements
- Change Management (Application/System)
- Changes in Healthcare Services
- Changes in Payor Mix
- Changes in Tax Law
- Charity Care
- Clinical Licensing/Medical Staff Credentialing
- Compensation & Benefits
- Competition – ACO, Population Management, Acute Care Hospitals, Physician-Owned Specialty Hospitals, Outpatient Facilities
- Compliance Comply Line
- Conflict of Interest
- Corporate Social Responsibility/Community Outreach
- Cost Reporting
- Data Center/Data Integrity Provisions
- Data Protection
- Database Administration
- Debt & Reserve Covenants
- Denial Management
- Development & Performance
- Disaster Recovery Testing
- Disbursement of Funds
- Document Retention
- EEOC/FMLA Compliance
- Employee Satisfaction
- Medical Records
- Medicare & Medicaid Regulations
- Billing
- Charge Capture
- Collections Management
- Contract Management
- Copay Collection
- Insurance Verification
- Medical Record (HIM) process for proper DRG & APC assignment
- Patient Access (Registration)
- Payment Posting
- Utilization/Case Management- Entry of Required Information
- Website Compliance
- Billing
- Charge Capture
- Coding and Compliance
- Collections Management
- Copay Collection
- Insurance Verification
- Patient Access (Registration)
- Payment Posting
- MOB Rentals
- Mobile Device Management
- Network/Perimeter Monitoring
- New Hire Processes
- On-Boarding Processes
- Operational and Business Planning
- Parking
- Patient Relations- Charge Dispute Complaints – Central Billing Office
- Patient Satisfaction – Quality of Care and Service
- Patient Valuables
- Payroll Cycle
- Employee Training
- Financial Reporting

- Fundraising
- Geographic Concentration
- Gift Shop
- Goodwill Impairment
- Governance Structure
- Health and Safety
- Healthcare Delivery Strategy
- HIPAA Regulatory Compliance
- Illegal Acts
- Incentives/Bonus – Merit increases, changes to salary/hourly rates, critical staffing bonus
- Incident Response
- Increasing Supply Costs
- Inpatient/Outpatient Billing Compliance
- Inventory Management
- Investments
- Journal Entry Procedures
- Labor Relations/ Union
- Liability & Insurance(s) – General, Malpractice, Directors & Officers, Cyber
- Litigation Risk
- Malpractice Accrual
- Manual check processes
- Marketing & Advertising
- Payroll Taxes
- Pension Funds
- Physical Security
- Physician Relationships/Referrals
- PIVOT Project and System Implementation – Epic
- Pricing & Quality Transparency
- Pricing Pressures – Managed Care, Governmental, Pharmaceutical, Quality-Based Reimbursement, and Payor risk
- Procurement/Purchasing
- Recording Time
- Recovery Audit Programs (RAC)
- Recruiting/Retention/Succession
- Regulatory Changes
- Research Grants & Clinical/Research Trials
- Resident Satisfaction
- Sanctioned Individuals
- Security Training and Awareness
- Segregation of Duties
- Social Media/Communications
- Strategic Vision and Planning
- Supply Shortages
- Tax Provision (Consideration for Exempt Organizations
- Termination Processes
- Third Party Payor Liabilities & Settlements – Central Billing Office
- Vendor Management

Risk Assessment Example – Risk Universe (IT)

Risk Universe

The scope of IT risk assessment included the following functional areas and processes within Organization:

- Disaster Recovery Plan
- Business Continuity Plan
- Business Impact Analysis
- Data Storage and Backup
- Risk Management
- Governance
- Vendor Management
- Capacity Management
- Physical Security
- Environnemental Controls
- Network/Perimeter Monitoring
- Data Protection
- Mobile Device Management
- User Management
- Incident Response
- Regulatory Compliance
- Security Training and Awareness
- Project Management
- Change Management- Application
- Change Management- System Software
- Change Management- Infrastructure
- Segregation of Duties

Leading Practices: Audit Planning

How To Integrate Risk Management Effectively for Audit Planning?

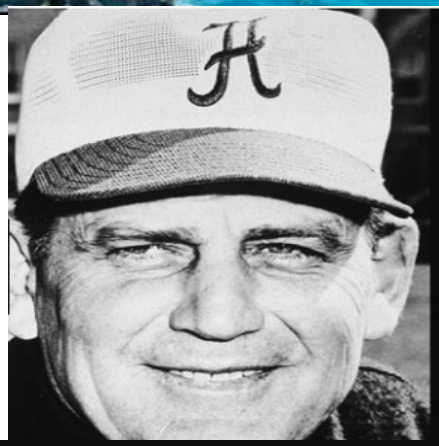
What is the MOST Significant Aspect of Developing an Audit Program

PLANNING

- Widely recognized as the most critical aspect in the setup, design, and even execution and reporting of audits

What Components Does Planning Include

- Define Audit Objectives
  - What are the Risks associated?
  - What criteria and/or metrics are involved?
- Define the Scope
  - Includes consideration of the extent & nature
- Research & Knowledge Gathering
  - Background, context, and initial documentation



Have a plan. Follow the plan, and you'll be surprised how successful you can be. Most people don't have a plan. That's why it's easy to beat most folks.

— Bear Bryant —

AZ QUOTES

Everyone has a plan 'till they get punched in the mouth.

— Mike Tyson —

Defining Audit Objectives and Scope

How Do You Do It?

Audit Objectives

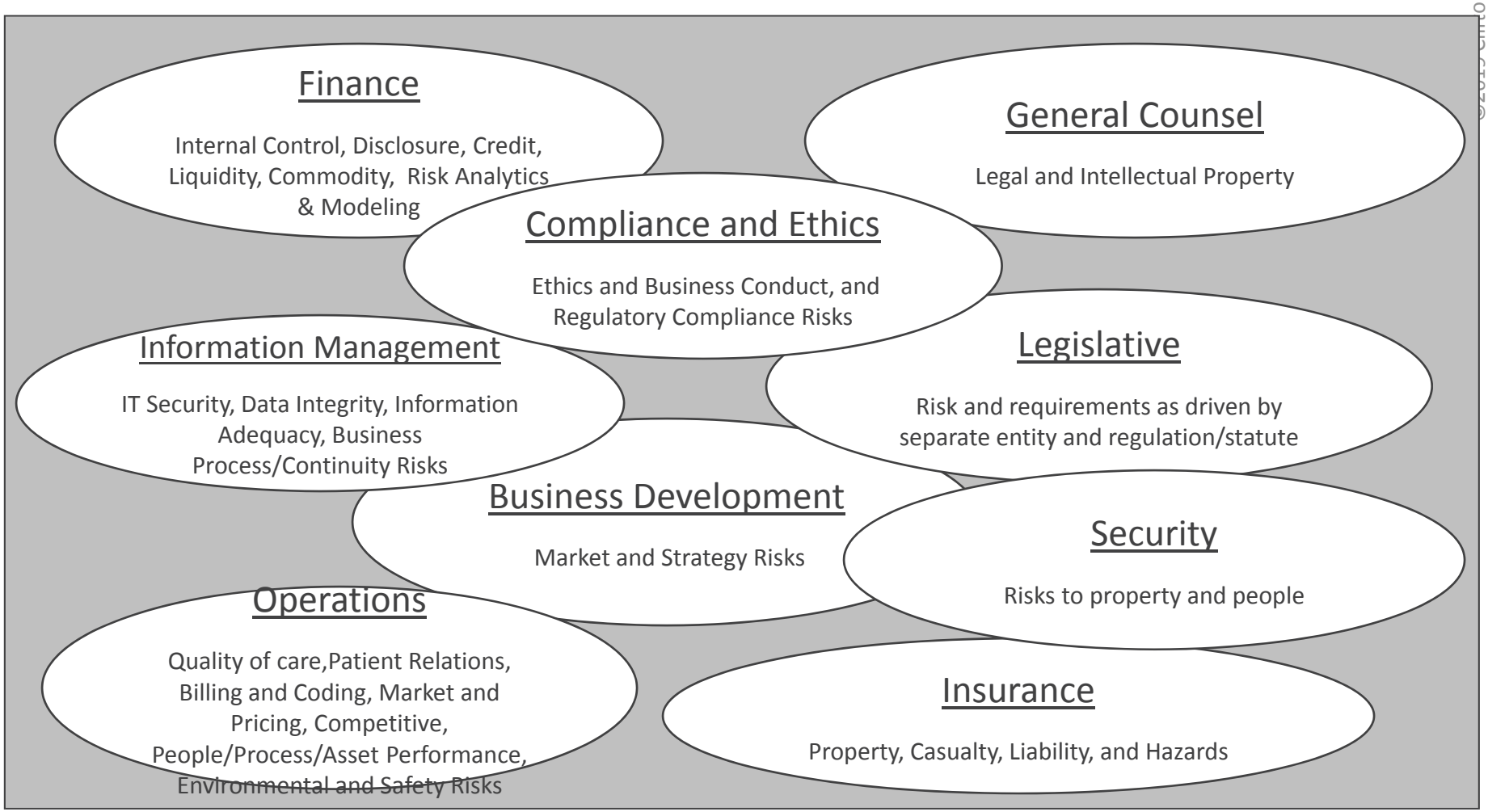
- Several Questions can help us truly assess the objectives of the audit:
  - What is “our” role?
  - What criteria and drivers exist for the audit? Why is the audit being performed (risks identified? Statute? Request?, etc.)
  - Who are the stakeholders and audience?
  - Are there known threats or concerns (fraud?, prior findings?, implementation issues?, etc.)

Audit Scope

Audit Scope

- What are the key processes and centers of operation?
- What is the timeline for the engagement and what period is in scope?
- What locations are included?
- What departments will be impacted?
- What metrics, measurements, and standards will be applied?

Scope?



Challenge is to align all these pieces into a common assessment & mold into audit planning

What Standards to Follow & Why?

- AICPA, GASB, OMB, etc. – highly prescriptive. Procedures are aligned and designed to achieve the criteria and requirements.
- Depending on the type of audit – utilizing the Institute of Internal Auditors (IIA) guidance for planning and development of audit programs is a valuable tool.
  - IIA 2200 – Planning. Must include resource allocations, objectives, scope, and timing in the audit program or separate planning documents.
  - IIA 2201 – Considerations. What risks are impacted/reviewed? How significant? What is management's control processes and effectiveness?
  - IIA 2210 – must have a risk assessment or conduct a prelim risk assessment of the activity/process/operation in scope. Must also incorporate procedures regarding fraud and noncompliance risks within the scope. Has adequate criteria and clear metrics been identified to measure test results?
  - IIA 2220 – Scope. Must identify the systems, records, personnel, and locations impacted by procedures. Are these included in the audit program steps and detail?

Audit Planning

Other Considerations:

- Separate Compliance from IA Planning?
  - Depends on culture and organizational structure
- Consider a rolling audit plan
  - Have a 3 year audit plan
    - Update the plan every 6 months
    - Still demonstrates consideration of other risks for the future
- Integrated Audit Opportunities?
  - Incorporate and integrate an IT and business/functional approach to the same audit
    - Not just entirely separate/disparate IT and operational/financial audits
- Build in flexibility
  - Allot time for unanticipated projects, issues, emerging risks

Questions?

CLAconnect.com

Jim Kreiser, CRMA, CISA, CFSA
Principal
Business Risk and Specialty Advisory Services
James.Kreiser@CLAConnect.com
215-643-3900