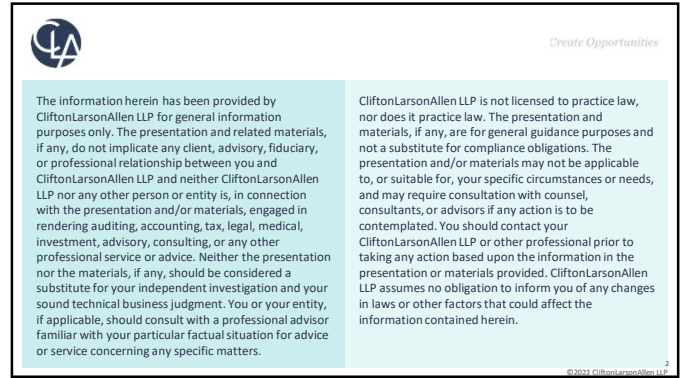
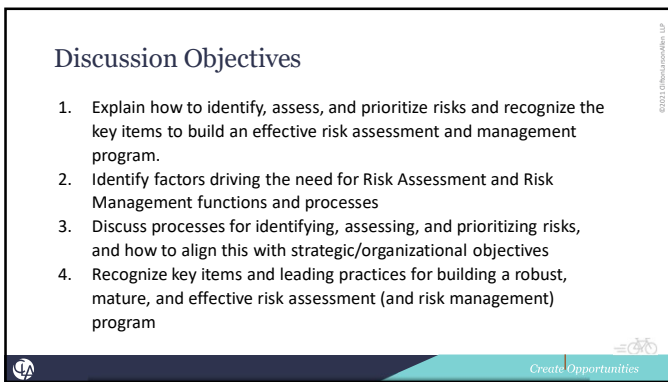




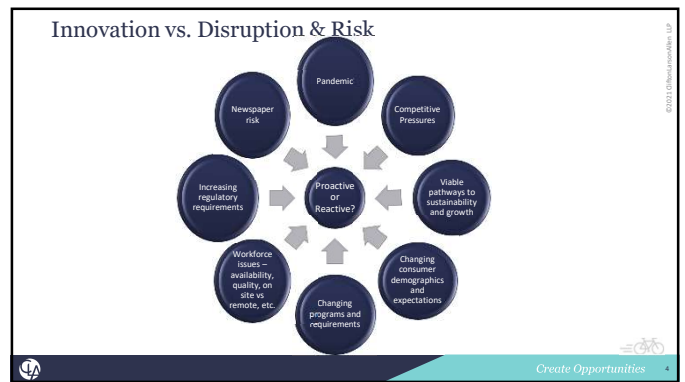
1



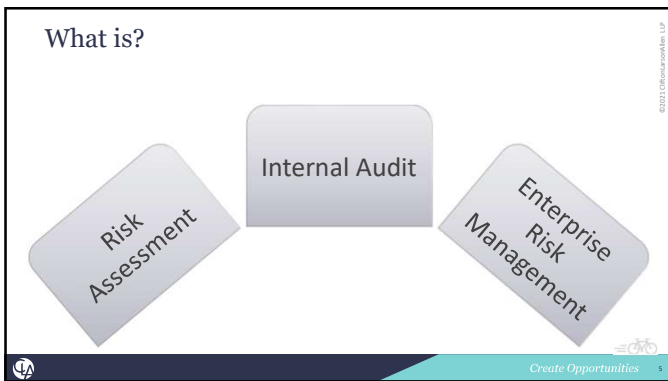
2



3



4



5



6

### What is Risk Assessment?

**Risk**

- Possibility that an event will occur and adversely affect achievement of objectives.

**Precondition to risk assessment**

- Establishment of objectives, linked at different levels of the entity.

**Risk assessment**

- Involves a dynamic and iterative process for identifying and assessing risks to the achievement of objectives.
- Forms basis for determining how risks will be managed.

7

### Benefits of Risk Management

Create 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

Retain/enhance board and executive trust and confidence in metrics/data

Protect and increase value for institution and your customers

Better align management decisions, investments, strategy, etc.

8

## Navigating Audit, Fraud, Compliance, and Risk

Factors Driving Risk Management

WEALTH ADVISORY | OUTSOURCING  
AUDIT, TAX, AND CONSULTING

Investment Advisory services are provided through CFAI Financial Advisor Wealth Advisors, LLC, which is a registered investment advisor.

9

### Key Perspectives on Risk & Compliance

**Figure 4—Convergence of Multiple Risk Factors in the Compliance Risk Ecosystem**

<https://www.cisr.ca.org/resources/area-studies/2019/volume-4/quarterly-compliance-risk-trends-and-tactics>

<https://cmfira.com/assets/uploads/images/MetricReasonM7.png>

10

### Fraud – Why Viewed Separately?

#### THE FRAUD TREE

OCCUPATIONAL FRAUD AND ABUSE CLASSIFICATION SYSTEM

2020 Report to the Nations. Copyright 2020 by the Association of Certified Fraud Examiners, Inc.

11

## Identifying, Assessing, and Prioritizing Risk:

How Do You Do It?

WEALTH ADVISORY | OUTSOURCING  
AUDIT, TAX, AND CONSULTING

Investment Advisory services are provided through CFAI Financial Advisor Wealth Advisors, LLC, which is a registered investment advisor.

12

### Think Differently....

Utilize an approach and framework that works for organization. Should integrate with management, board, and objectives.

**Illustrative Model:**

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

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

Create Opportunities

13

### Progression to Integrate Risk Management

- Risk and Audit need to evolve. IIA and other recent studies emphasize how risk assessments as lists/grids simply lose buy-in and value.
- What role can we play to integrate some of these disparate functions?
- How do we enhance and create creditability and sustainability in audit efforts? Risk Assessments simply can't be once-a-year lists.

Create Opportunities

14

### Risk Integration with Opportunities!

Create Opportunities

15

### Progression to Integrate Risk Management

**Phase I: Buy-In. Understand, accept, commit to pilot**

- Value Proposition
- Clarify RM needs & expectations
- Executive awareness and commitment
- Agree on scope, criteria, process
- Establish RM as a priority
- Communicate

**Phase II: Assess risks and risk management capability**

- Set risk appetite & key performance metrics
- Assess vulnerability to selected key risks
- Quality before quantify
- Assess interactions and risk experience
- Assess current capabilities
- Develop risk profile
- Identify gaps & prioritize

Create Opportunities

16

### Progression to Integrate Risk Management

**Phase III: Detailed recommendations to resolve capability gaps in effectiveness**

- Define authorities, requirements, resources
- Design sustainable process
- Identify capabilities for design
- Design change management
- Proof of Concept
- Decision to proceed

**Phase IV: Implement, Operate & Continuously Improve.**

- Deploy tools
- Train personnel
- Monitor & Report
- Integrate into core management processes
- Change management
- Continuously improve

Create Opportunities

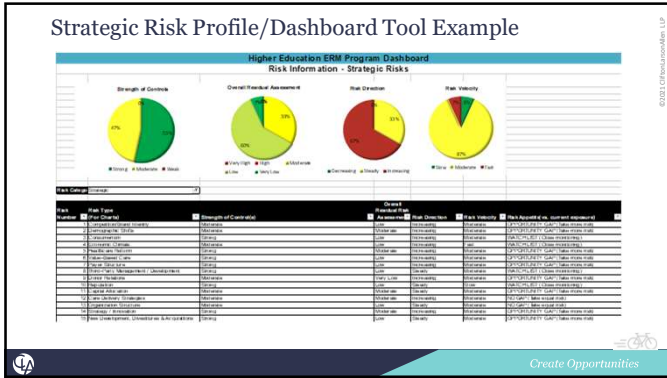
17

### The DNA of the Risk Intelligent Organization

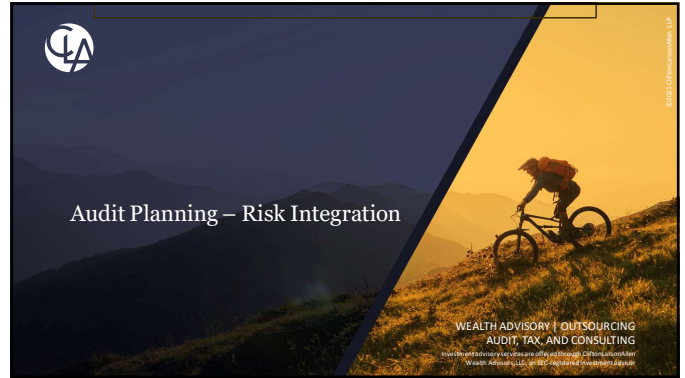
Risk intelligence is embedded in the Risk-Informed decision-making process, such as Business Planning and Capital Allocation, and improves preparedness for adverse events

Create Opportunities

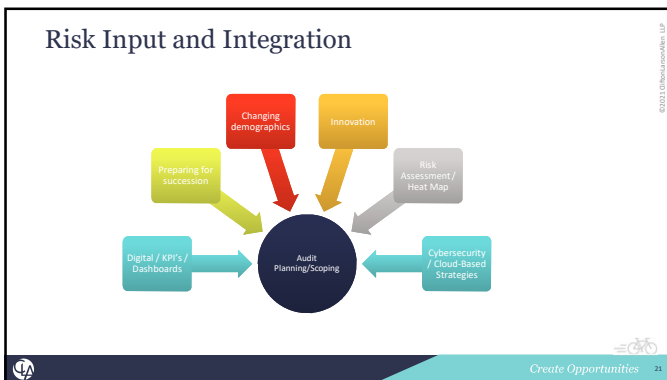
18



19



20



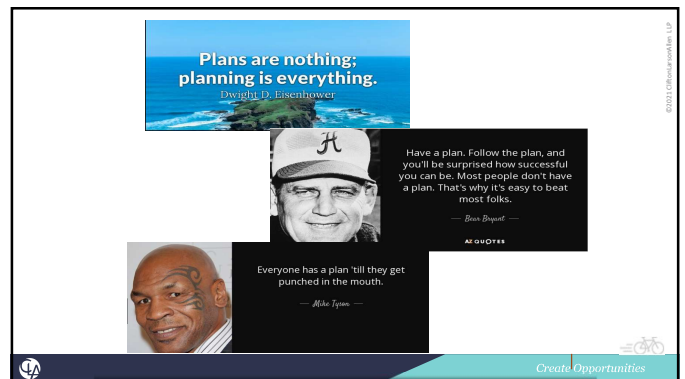
21

- ### 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.)**

22

- ### 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

23



## Audit Scope



25

## What Are My Procedures?

- What testing are you including in the audit program? How is your sampling going to be driven? AICPA, FDICIA, NCUA, risk based?, judgmental?. Sampling criteria should be documented and included in the audit program.
- Is the focus of the audit governance or design or effectiveness or all of the above? What procedures and testing need to be in place to achieve the audit objectives and satisfy the scope?
- Sampling – as well as Audit Evidence – will be discussed in further detail later today. However, these are critical areas to contemplate and consider when establishing your procedures and testing.

26

## What Standards to Follow & Why?

- AICPA, FASB, NCUA, GAAP, IT (CSF, ISO, other), etc. – can be 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?

27

## Case Studies - Discussion

*Implementation, Practices, and Complexities*

WEALTH ADVISORY | OUTSOURCING  
AUDIT, TAX, AND CONSULTING

28

## What Is the Proper Risk Universe?

- What are the expectations involved in the extent (number) of discreet risks at an organization?
  - Can be quite extensive
  - Can be “middle of the road”
  - Can be quite limited

29

## What Is the Proper Risk Universe?

- Have you seen risks defined this way? Client uses this as a model...
  - Strategic Risk
  - Operational Risk
  - Financial Risk
  - Human Capital (HR)
  - Information Technology (IT)
  - Regulatory/Compliance
  - Reputational
    - Nuance of client culture for ownership to executives/managers for all risk

30

Example – What About This? (higher ed client)

Strategic (S)	Operational (O)	Financial (F)	Human Capital (H)	Legal/Regulatory (L/R)	Technology (T)
1. Competition/Brand Identity	14. Operations - Planning	27. Performance Management	33. Leadership	47. Contracts & Security	54. Data Relevance & Integrity
2. Demographic Shifts	15. Database/Analytics	28. Budgeting/Planning	34. Skills/Competency	48. Privacy & Security	55. IT Infrastructure/Architecture
3. Customer Expectations	16. Process Execution	29. Capital Structure	35. Succession Planning	49. Liability	
4. Economic Climate	17. Interdependency	30. Accounting/ Tax Information	36. Diversity	50. Accreditation	56. IT Reliability/ Recovery
5. Business Model Disruption	18. Change Integration	31. External Reporting & Disclosure	37. Labor Shortage	51. Regulatory Environment	57. IT Security/ Cyber-risk
6. Partnerships/ Affiliates	19. Customer Satisfaction	32. Liquidity	38. Performance Incentives	52. Legal/Regulatory Compliance	58. IT Change Controls
7. Donor Relations	20. Resource Capacity/ Allocation		39. Change Readiness	53. Fraud & Abuse	59. Access Controls
8. Reputation	21. Knowledge/ Intellectual Capital		40. Cultural Health	41. Communication	60. Systems Implementation
9. Capital Allocation	22. Channel Effectiveness		42. Employee Engagement	43. Accountability	
10. Education Delivery Strategies	23. Student/Faculty Safety		44. Labor Relations (Union)		
11. Organization Structure	24. Vendor/ Outsourcing				
12. Organizational Policies	25. Facilities/Power Change				
13. Strategy/Innovation					

1. Common Risk Language (What does "risk" mean to our organization?)

2. COVID-19 Risk Impacts (How is our risk profile changing?)

3. "Risk Streams" = (What risk dynamics exist across risks?)

4. Risk Gaps - Appetite vs. Exposure (Where do we need to take res/more risk?)

31

What Is the Proper Risk Universe?

- Is 7 risks appropriate?
  - Probably not. 5-7 Risk Categories may be appropriate, but likely need more depth and context to adequately manage/report risks.
  - Is 60 risks too many?
  - What about 125?.....

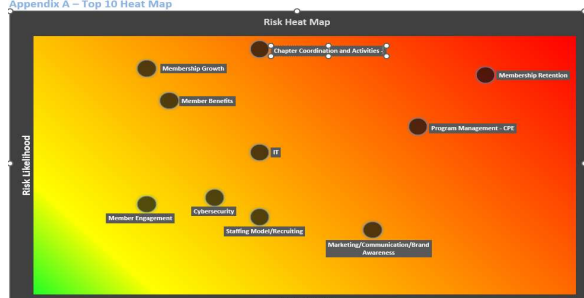
32

Healthcare Risk Universe

Strategic	Operational	Financial	Regulatory/Compliance
<b>Core Competencies:</b> <ul style="list-style-type: none"> <li>Board performance</li> <li>Focus of the top</li> <li>Control environment</li> <li>Consumer benefits</li> <li>Corporate sustainability</li> <li>Reputational risks</li> </ul> <b>Strategy &amp; Major Initiatives:</b> <ul style="list-style-type: none"> <li>Mission, values, culture</li> <li>Planning, execution and integration</li> <li>Change management</li> <li>Measurement and monitoring</li> <li>Tech implementation and support</li> </ul> <b>Planning and Resource Allocation:</b> <ul style="list-style-type: none"> <li>Strategic planning</li> <li>Capital planning</li> <li>Physical relationships</li> <li>Partnerships &amp; JVs</li> <li>Payer relationships</li> <li>Annual budgeting &amp; forecasting</li> <li>Outsourcing engagements</li> </ul> <b>Market Forces:</b> <ul style="list-style-type: none"> <li>Healthcare reform</li> <li>Payer mix</li> <li>Consolidation / retail</li> <li>Demographic and lifestyle trends</li> <li>Accessibility and affordability</li> <li>Value based care</li> </ul> <b>Managers, Executives, Oversight:</b> <ul style="list-style-type: none"> <li>Due diligence</li> <li>Valuation and pricing</li> <li>Execution and integration</li> <li>ROI monitoring</li> </ul> <b>Stakeholder Relationships / Communication:</b> <ul style="list-style-type: none"> <li>Regulatory and government affairs</li> <li>Rating agencies</li> <li>Media relations</li> <li>Investor communication</li> <li>Community sustainability</li> </ul>	<b>People:</b> <ul style="list-style-type: none"> <li>Recruitment, retention, termination</li> <li>Training, development, performance management</li> <li>Compensation &amp; benefits</li> <li>Staff engagement</li> <li>Succession planning</li> </ul> <b>Care Delivery:</b> <ul style="list-style-type: none"> <li>Quality, safety, service, access, affordability</li> <li>Utilization, V/Q/D, HAP</li> <li>Top of scope practice</li> <li>Enabling technology</li> <li>Pricing &amp; performance</li> </ul> <b>Information Technology:</b> <ul style="list-style-type: none"> <li>IT management, infrastructure, integrity</li> <li>IT security / access</li> <li>IT reliability / continuity</li> </ul> <b>Physical Assets:</b> <ul style="list-style-type: none"> <li>Related to property, plant, equipment</li> <li>Real estate</li> <li>Lease / lease of assets</li> </ul> <b>Supply Chain:</b> <ul style="list-style-type: none"> <li>Procurement and distribution management</li> <li>Inventory and distribution planning</li> <li>Autosure monitoring</li> <li>Contractual relationships</li> </ul> <b>Sales and Marketing:</b> <ul style="list-style-type: none"> <li>Value Based Reimbursement</li> <li>Advertising and marketing</li> <li>Debtser preparedness</li> <li>Business continuity planning</li> </ul> <b>Research and Health Education:</b> <ul style="list-style-type: none"> <li>Grant compliance</li> <li>Conflict of interest policy</li> <li>Other research oversight</li> <li>Medical school relationships</li> </ul>	<b>Revenue Cycle:</b> <ul style="list-style-type: none"> <li>Payer contracting</li> <li>Registration and scheduling</li> <li>Charge capture integrity</li> <li>Coding and documentation</li> <li>Billing, collections, denial management</li> <li>Credit balance monitoring</li> <li>CDM maintenance / strategic pricing</li> <li>Bad debt and merged care reserves</li> </ul> <b>Accounting and Reporting:</b> <ul style="list-style-type: none"> <li>Accounting, reporting and disclosures</li> <li>Debt structure / levels</li> <li>Operational sustainability</li> <li>Internal control / SOX</li> <li>Major accounting estimates</li> <li>Bad debt and merged care reserves</li> <li>Malpractice reserves</li> <li>Cost reports</li> </ul> <b>Liquidity and Credit:</b> <ul style="list-style-type: none"> <li>Cash management</li> <li>Capital funding</li> <li>Inventory turnover</li> <li>Portfolio management / risk</li> <li>Credits and collections</li> <li>Insurance</li> </ul> <b>Capital Structure:</b> <ul style="list-style-type: none"> <li>Debt</li> <li>Equity</li> <li>Warrant funds</li> <li>Stock options</li> <li>Dividends</li> </ul> <b>Tax:</b> <ul style="list-style-type: none"> <li>Maintain 501(c)(3) status</li> <li>Tax compliance and audit management / JALF</li> <li>Tax strategy and planning</li> <li>Tax optimization</li> </ul>	<b>Regulatory:</b> <ul style="list-style-type: none"> <li>Compliance management</li> <li>ODG work plan</li> <li>Code of conduct</li> <li>Anti-protection and security</li> <li>Labor laws</li> <li>Anti-trust / anticompetition</li> <li>EMR/HLA</li> <li>Sanctioned individuals</li> <li>Payment card industry (PCI) compliance</li> <li>Environmental regulations</li> <li>Securities regulations</li> <li>Healthcare and safety regulations</li> </ul> <b>Legal:</b> <ul style="list-style-type: none"> <li>Contracts</li> <li>Claims</li> <li>Malpractice liability</li> <li>Vendor assessment</li> <li>Insurance and risk management</li> <li>HIPAA</li> </ul>

33

How Best to Display Key Risks?



34

How Best to Display Key Risks?

Risk	Level of documented control procedures	Size or volume	New products, services, or processes systems	Personal turnover and risk	Complexity	Susceptibility to fraud	Information and reporting	Length of time since the area was reviewed	Volume and severity of issues previously	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 Payer 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,	2.00	4.00	4.00	1.00	3.00	1.00	3.00	5.00	1.00	2.45
7. Licensing/Certification	1.00	4.00	1.00	4.00	3.00	1.00	3.00	5.00	1.00	2.45
8. Labor Relations/ Union										

35

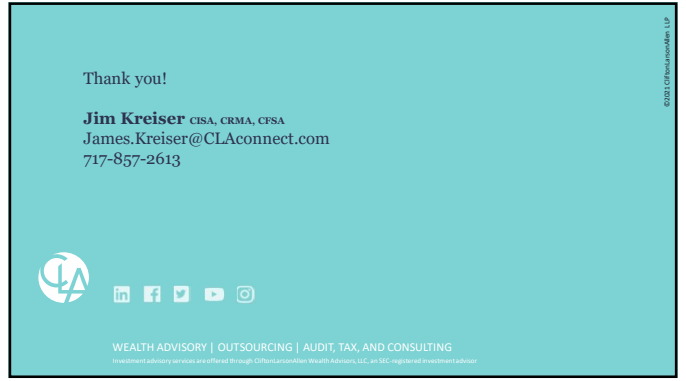
Impact of Colors & Format & Reporting

- Couple client anecdotes as cautionary tales
  - Misinterpreting Risk Assessment for Findings/Audit
  - Colors – Red = Bad? Green = Good? No color
    - My area is better than Patrick's – so he should be red...
  - Coordination of Action Plans?
    - Provided action plans recommendations – met with pushback.

36



37



38