Government - 2023

Effective Risk Assessment, Risk Management and Audit Planning

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

The information herein has been provided by CliftonLarsonAllen LLP for general information purposes only. The presentation and related materials, if any, do not implicate any client, advisory, fiduciary, or professional relationship between you and CliftonLarsonAllen LLP and neither CliftonLarsonAllen LLP nor any other person or entity is, in connection with the presentation and/or materials, engaged in rendering auditing, accounting, tax, legal, medical, investment, advisory, consulting, or any other professional service or advice. Neither the presentation nor the materials, if any, should be considered a substitute for your independent investigation and your sound technical business judgment. You or your entity, if applicable, should consult with a professional advisor familiar with your particular factual situation for advice or service concerning any specific matters.

CliftonLarsonAllen LLP is not licensed to practice law, nor does it practice law. The presentation and materials, if any, are for general guidance purposes and not a substitute for compliance obligations. The presentation and/or materials may not be applicable to, or suitable for, your specific circumstances or needs, and may require consultation with counsel, consultants, or advisors if any action is to be contemplated. You should contact your CliftonLarsonAllen LLP or other professional prior to taking any action based upon the information in the presentation or materials provided. CliftonLarsonAllen LLP assumes no obligation to inform you of any changes in laws or other factors that could affect the information contained herein.

Discussion Objectives

1. Explain how to identify, assess, and prioritize risks and recognize the key items to build an effective risk assessment and management program.
2. Identify factors driving the need for Risk Assessment and Risk Management functions and processes
3. Discuss processes for identifying, assessing, and prioritizing risks, and how to align this with strategic/organizational objectives
4. Recognize key items and leading practices for building a robust, mature, and effective risk assessment (and risk management) program

Innovation vs. Disruption & Risk

What is?

What is Enterprise Risk Management (ERM)?

Process designed to:

Identify potential events that may affect the entity,	Manage risk to be within the risk appetite, and to	Provide reasonable assurance regarding achievement of objectives.

↓

SHOULD include:

Board of directors,	Management, and	Other personnel

↓

Applied in strategy-setting and across the enterprise.

What is Risk Assessment?

Risk

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

Risk assessment

Precondition to risk assessment

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

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.

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.**	

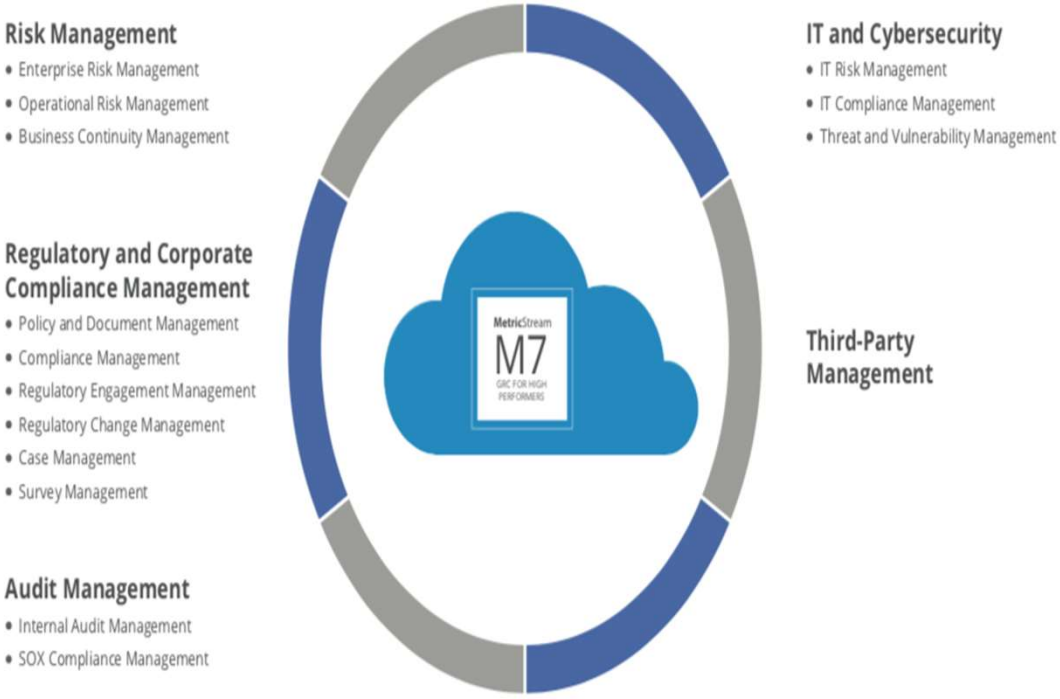
Navigating Audit, Fraud, Compliance, and Risk

Factors Driving Risk Management

WEALTH ADVISORY | OUTSOURCING
AUDIT, TAX, AND CONSULTING

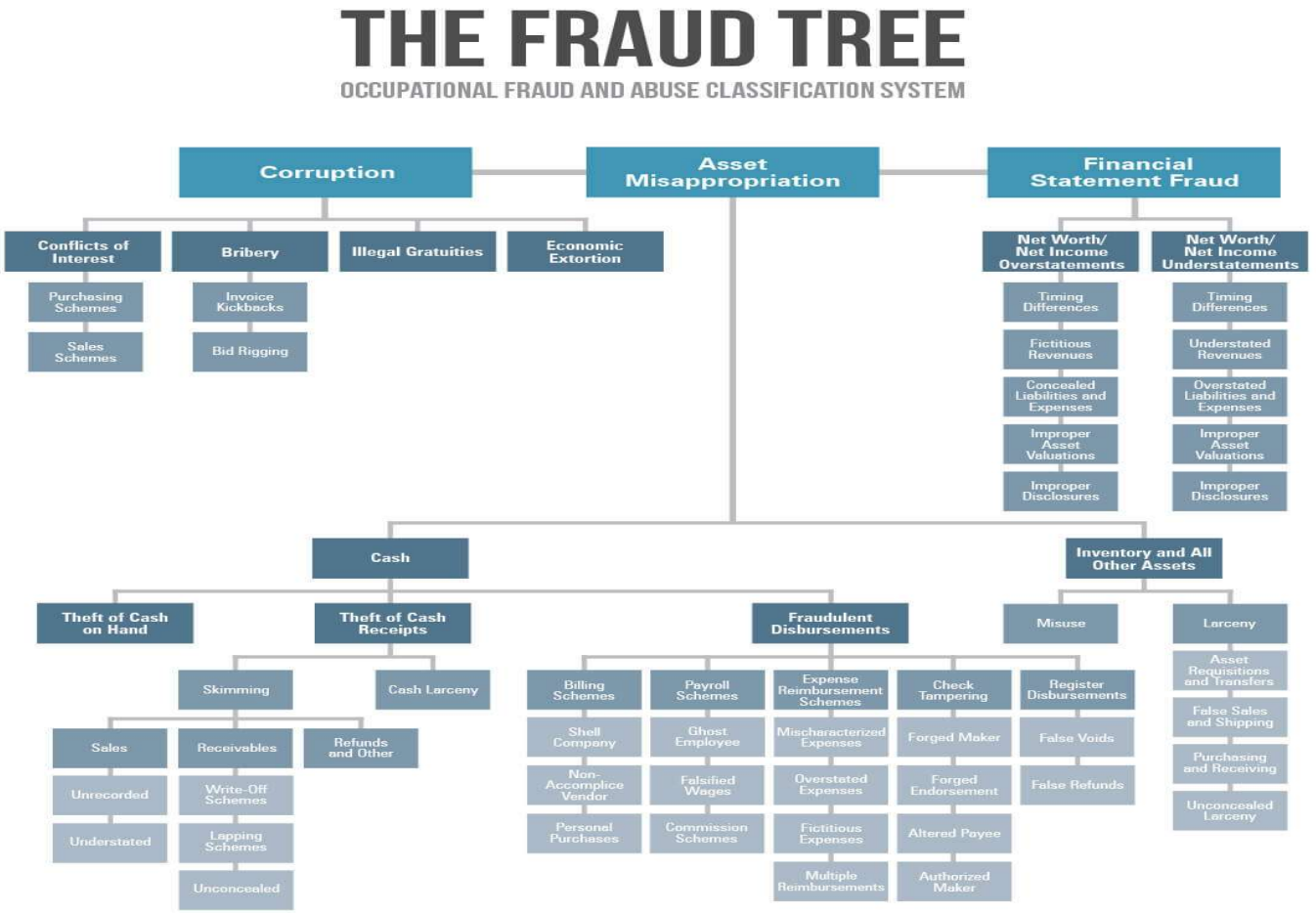
Key Perspectives on Risk & Compliance

https://www.isaca.org/resources/isaca-journal/issues/2019/volume-4/understanding-compliance-risk-in-finance-and-banking



https://ctmfile.com/assets/ugc/images/MetricStreasmM7.png

Fraud – Why Viewed Separately?



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

Identifying, Assessing, and Prioritizing Risk:

How Do You Do It?

WEALTH ADVISORY | OUTSOURCING
AUDIT, TAX, AND CONSULTING

Think Differently….

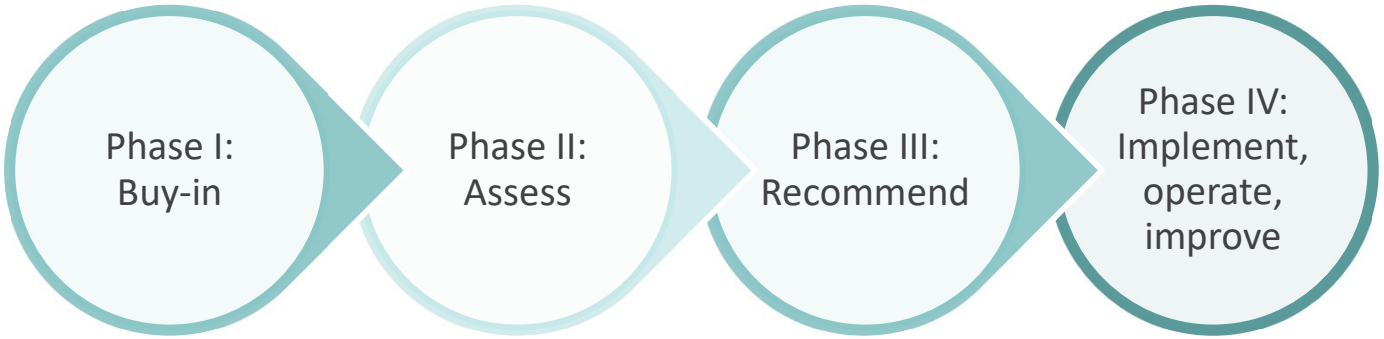
Utilize an approach and framework that works for organization. Should integrate with management, board, and objectives.

Illustrative Model:

- Level of Control Documentation and Governance
- Size or Volume of Transactions/Accounts
- New Products or Systems
- Personnel Quals 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

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.

Risk Integration with Opportunities!

How often do we truly assess strengths and opportunities?

- Risk Management often includes focus on "weakness and threats"

SWOT Analysis

Strengths, Weakness, Opportunities, and Threats

Integrate into ERM approach in order to better invest, capitalize, and differentiate organization!

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
- Qualify before quantify
- **Assess interactions and risk experience**
- Assess current capabilities
- **Develop risk profile**
- **Identify gaps & prioritize**

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

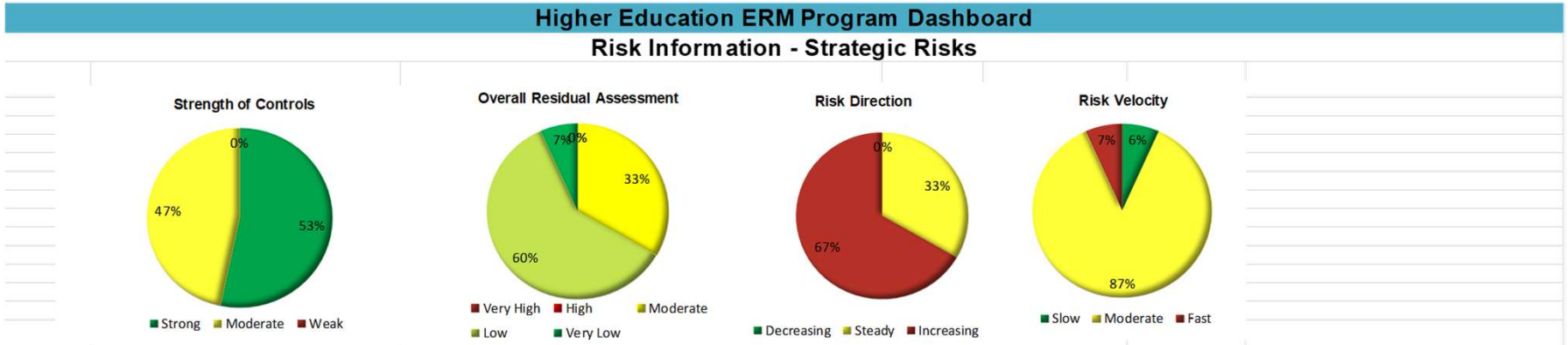
Phase IV: Implement, Operate & Continuously Improve.

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

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

Strategic Risk Profile/Dashboard Tool Example



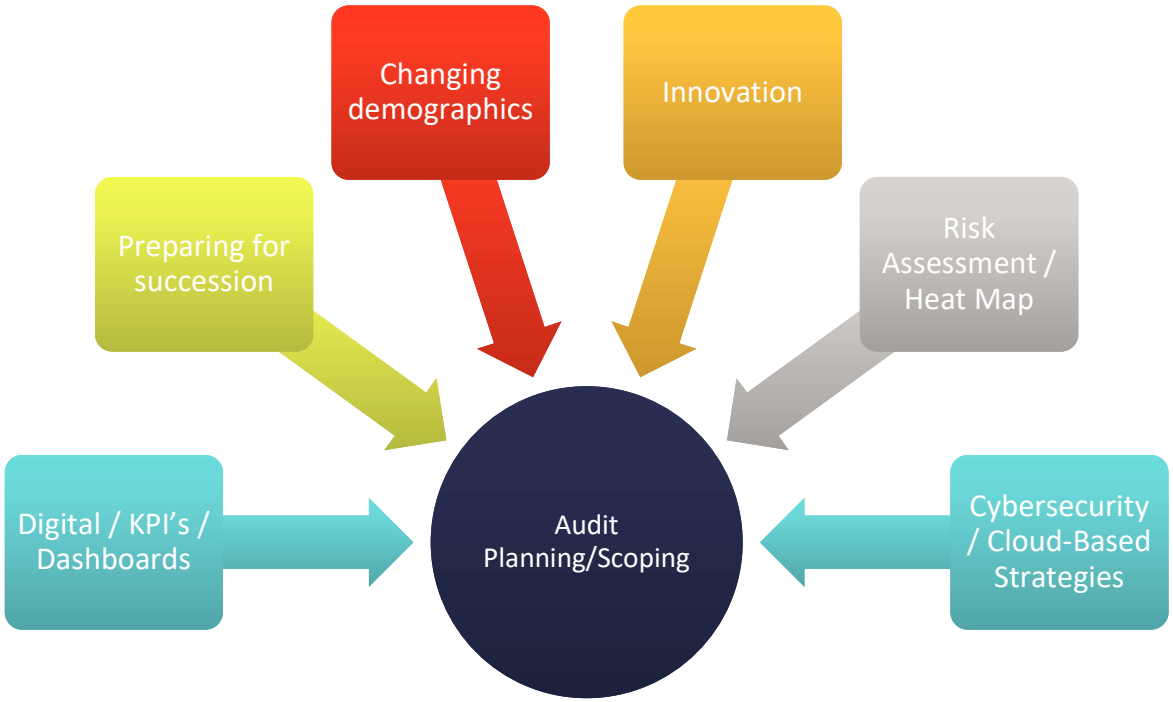
Risk Catego Strategic

Risk Number	Risk Type (For Charts)	Strength of Control(s)	Overall Residual Risk Assessmer	Risk Direction	Risk Velocity	Risk Appetite(vs. current exposure)
1	Competition/Brand Identity	Moderate	Low	Increasing	Moderate	OPPORTUNITY GAP (Take more risk)
2	Demographic Shifts	Moderate	Moderate	Increasing	Moderate	OPPORTUNITY GAP (Take more risk)
3	Consumerism	Strong	Low	Increasing	Moderate	WATCH LIST (Close monitoring)
4	Economic Climate	Moderate	Low	Increasing	Fast	WATCH LIST (Close monitoring)
5	Healthcare Reform	Strong	Moderate	Increasing	Moderate	OPPORTUNITY GAP (Take more risk)
6	Value-Based Care	Strong	Low	Increasing	Moderate	OPPORTUNITY GAP (Take more risk)
7	Payer Structure	Strong	Low	Increasing	Moderate	OPPORTUNITY GAP (Take more risk)
8	Third-Party Management / Development	Strong	Low	Steady	Moderate	WATCH LIST (Close monitoring)
9	Donor Relations	Moderate	Very Low	Increasing	Moderate	OPPORTUNITY GAP (Take more risk)
10	Reputation	Strong	Low	Steady	Slow	WATCH LIST (Close monitoring)
11	Capital Allocation	Moderate	Moderate	Steady	Moderate	OPPORTUNITY GAP (Take more risk)
12	Care Delivery Strategies	Moderate	Moderate	Increasing	Moderate	NO GAP (Take equal risk)
13	Organization Structure	Moderate	Low	Steady	Moderate	NO GAP (Take equal risk)
14	Strategy / Innovation	Strong	Moderate	Increasing	Moderate	OPPORTUNITY GAP (Take more risk)
15	New Development, Divestitures & Acquisitions	Strong	Low	Steady	Moderate	OPPORTUNITY GAP (Take more risk)

Audit Planning – Risk Integration

WEALTH ADVISORY | OUTSOURCING
AUDIT, TAX, AND CONSULTING

Risk Input and Integration

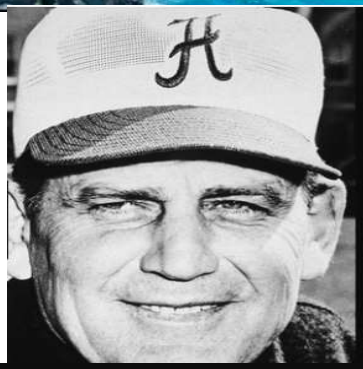


Questions Auditors Should Ask About the RA

- 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.)***

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 —

Audit Scope

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.

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?

Case Studies - Discussion

Implementation, Practices, and Complexities

WEALTH ADVISORY | OUTSOURCING
AUDIT, TAX, AND CONSULTING

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

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

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	54. Data Relevance & Integrity
2. Demographic Shifts	15. Process Quality	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	56. IT Reliability/ Recovery
4. Economic Climate	17. Interdependency	30. Accounting/ Tax Information	36. Diversity	50. Accreditation Agencies	57. IT Security/ Cyber-risk
5. Business Model Disruption	18. Change Integration	31. External Reporting & Disclosure	37. Labor Shortage	51. Regulatory Environment	58. IT Change Controls
6. Partnerships/ Affiliates	19. Customer Satisfaction	32. Liquidity	38. Performance Incentives	52. Legal/ Regulatory Compliance	59 Access Controls
7. Donor Relations	20. Resource Capacity/ Allocation		39. Change Readiness	53. Fraud & Abuse	60. Systems Implementation
8. Reputation	21. Knowledge/ Intellectual Capital		40. Cultural Health		
9. Capital Allocation	22. Channel Effectiveness		41. Communication		
10. Education Delivery Strategies	20. Student/Faculty Safety		42. Employee Engagement		
11. Organization Structure	25. Vendor/ Outsourcing		43. Accountability		
12. Organizational Policies	26. Facilities/Power Outage		44. Labor Relations (Union)		
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 less/more risk?)

What Is the Proper Risk Universe?

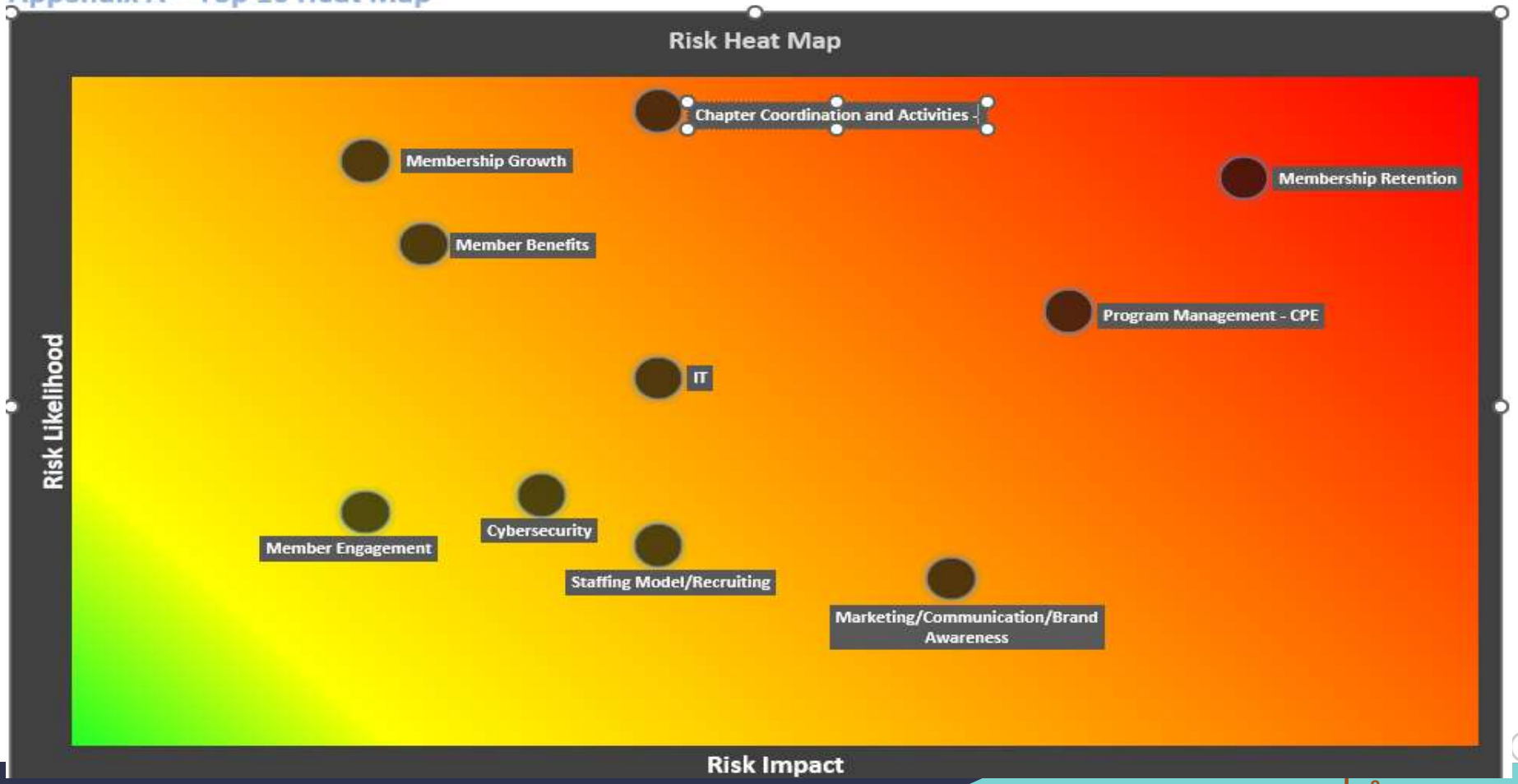
- Is 7 risks appropriate?
  - Probably not. 5-7 Risk Categories may be appropriate, but likely need more depth and context to adequately manage/report risks.
  - Is 60 risks too many?
  - What about 125?.....

Healthcare Risk Universe

Strategic	Operations	Financial	Regulatory/Compliance
Governance: ► Board performance ► Tone at the top ► Control environment ► Community benefit ► Corporate sustainability ► Reputational risks ► Management fraud **Strategy & Major Initiatives:** ► Mission, values, culture ► Planning, execution and integration ► Change management ► Measurement and monitoring ► Tech implementation and support **Planning and Resource Allocation:** ► Organizational structure ► Strategic planning ► Capital planning ► Physician relationships ► Partnerships & JV's ► Payer relationships ► Annual budgeting & forecasting ► Outsourcing arrangements **Market Forces:** ► Healthcare reform ► Payer mix ► Competition ► Consumerism / retail ► Demographic and lifestyle trends ► Accessibility and affordability ► Value based care **Mergers, Acquisitions, Divestitures:** ► Due diligence ► Valuation and pricing ► Execution and integration ► ROI monitoring **Stakeholder Relationships / Communication:** ► Regulatory and government affairs ► Rating agencies ► Media relations ► Employee communication ► Corporate sustainability	**People:** ► Culture ► Recruitment, retention, termination ► Training, development, performance management ► Labor relations ► Compensation & benefits ► Staff engagement ► Succession planning **Care Delivery:** ► Quality, safety, service, access, affordability ► Utilization, TCOC, P4P ► Top of scope practice ► Enabling technology ► Pricing & partnerships ► Care delivery network **Information Technology:** ► IT management, infrastructure, integrity ► IT security / access ► IT availability / continuity **Physical Assets:** ► Reinvest in property, plant, equipment ► Real estate ► Loss / theft of assets **Supply Chain:** ► Procurement ► Inventory and distribution management ► Rebate monitoring ► Variation reduction and planning **Sales and Marketing:** ► New business development ► Advertising and marketing **Emergency Management:** ► Disaster preparedness ► Biohazards ► Business continuity planning **Research and Health Education:** ► Grant compliance ► Conflict of interest policy ► Peer review oversight ► Medical school relationships	**Revenue Cycle:** ► Payer contracting ► Registration and scheduling ► Charge capture integrity ► Coding and documentation ► Billing, collections, denials management ► Credit balance monitoring ► CDM maintenance / strategic pricing ► Bad debt and charity care **Accounting and Reporting:** ► Accounting, reporting and disclosures ► Debt structure / levels ► Department accountability ► Internal control / SOX ► Major accounting estimates ► Bad debt and managed care reserves ► Malpractice reserves ► Cost reports **Liquidity and Credit:** ► Cash management ► Capital funding ► Inventory turnover ► Portfolio management / risk ► Credit and collections ► Insurance **Capital Structure:** ► Debt ► Equity ► Pension Funds ► Stock options ► Liquidity pressure **Tax:** ► Maintain 501(c)3 status ► Tax compliance and audit management / SALT ► Tax strategy and planning ► Tax optimization	**Regulatory:** ► Compliance management ► OIG work plan ► Code of conduct ► Data protection and security ► Labor laws (EEOC/FMLA) ► Anti-Trust / unfair competition ► EMTALA ► Sanctioned individuals ► Payment card industry (PCI) compliance ► Environmental regulations ► Securities regulations ► Healthcare and safety regulations **Legal:** ► Contracts ► Claims ► Malpractice liability ► Vendor assessment ► Insurance and risk management ► HIPAA

How Best to Display Key Risks?

Appendix A – Top 10 Heat Map



How Best to Display Key Risks?

Risk Assessment Results

	Risk	Level of documented control procedures (15%)	Size or volume (10%)	New products, services, or processing systems (10%)	Personnel turnover and mix (15%)	Complexity (10%)	Susceptibility to fraud (10%)	Information and reporting (10%)	Length of time since the area was reviewed (10%)	Volume and severity of issues previously identified	Total Score (100%)
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

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.

Questions

Thank you!

Jim Kreiser CISA, CRMA, CFSA
James.Kreiser@CLAconnect.com
717-857-2613

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING