A Practical & Tactical Approach to Implementing Enterprise Risk Management (ERM)

National Society of Accountants for Cooperatives (NSAC)

Jennifer Leary, Partner – National Risk Management

Speaker Bio – Jen Leary

Jennifer (Jen) Leary, CPA, National Partner – Risk Management for CliftonLarsonAllen

Jen is a National technical partner in CLA's Business Risk Services consulting practice. She has more than 16 years of experience serving clients in a variety of industries on both internal and external audit engagements and in various consulting roles.

Her professional background includes over a decade with an international accounting firm serving clients in the U.S. and throughout Europe and Asia. She is also a noted speaker on various topics and trainer of our internal and external teams including Enterprise Risk Management , Internal Controls Process Improvement, Contract Compliance and Acquisitions Consulting.

Agenda Topics

1. Briefly summarize ERM *(the "technical")*
2. Understanding the ERM maturity model and where you may fit *(the "practical")*
3. Developing an action plan for implementation *(the "tactical")*
4. Questions & Answers

PART ONE OF FOUR

Briefly summarize ERM

(the "technical")

Why Discuss ERM?

All entities face inherent risk and uncertainty, and the challenge for management is to determine what level of risks to accept as it strives to grow and deliver value, and what costs to incur to manage/mitigate risks throughout the process.

What Is Risk Governance?

Directors and management evaluating, monitoring and improving their processes for overseeing the company's framework of risk assessment and risk management activities.

Increasing Demand for Enhanced Governance and Risk Oversight

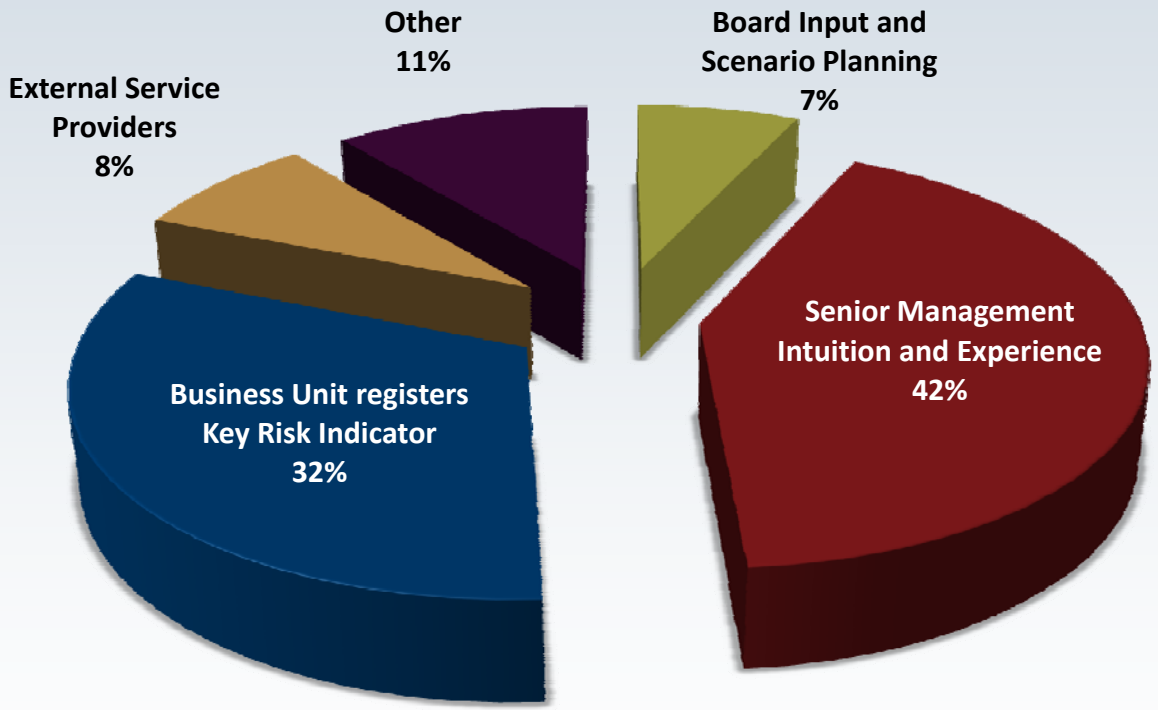
- **2012 Dodd-Frank Act Rules**
  - compensation committee independence
  - disclosure of pay-for-performance, pay ratios, and hedging by employees and directors
  - recovery of executive compensation
  - reporting over conflict minerals essential for business
  - disclosure of government payments to resource extraction issuers, companies engaging in commercial development of oil, natural gas, and minerals
- **2010 SEC Rules to Enhance Corporate Governance Disclosures**
  - director and nominee qualifications and legal proceedings
  - diversity and director nominations
  - board leadership structure and role in risk oversight
  - accelerated disclosure of shareholder voting results
- **COSO – Enterprise Risk Management Framework**
  - Provides an organizational scope, emphasis, and program to broaden risk management to an enterprise-wide emphasis and integrate into corporate strategy
- **Sarbanes-Oxley, 2002**
  - Calls for enterprise-wide documentation and testing of controls over financial reporting risk

Many organizations' response is to enhance their corporate governance processes by developing and implementing an Enterprise Risk Management process

Evaluating Risk Information: AON 2011 Survey

Source: www.aon.com

Industry Sources of Identified Risk



CliftonLarsonAllen

Risk Information – AON Survey Source: www.aon.com

Top 10 Risks Facing Organizations:

1. Economic Slowdown
2. Regulatory/legislative changes
3. Increased competition
4. Damage to reputation and brand
5. Business interruption
6. Failure to innovate/meet customer needs
7. Failure to attract or retain top talent
8. Commodity price risk
9. Technology failure/system failure
10. Cash flow/liquidity risk

PART TWO OF FOUR

Understanding the ERM maturity model and where you may fit

(the "practical")

CliftonLarsonAllen

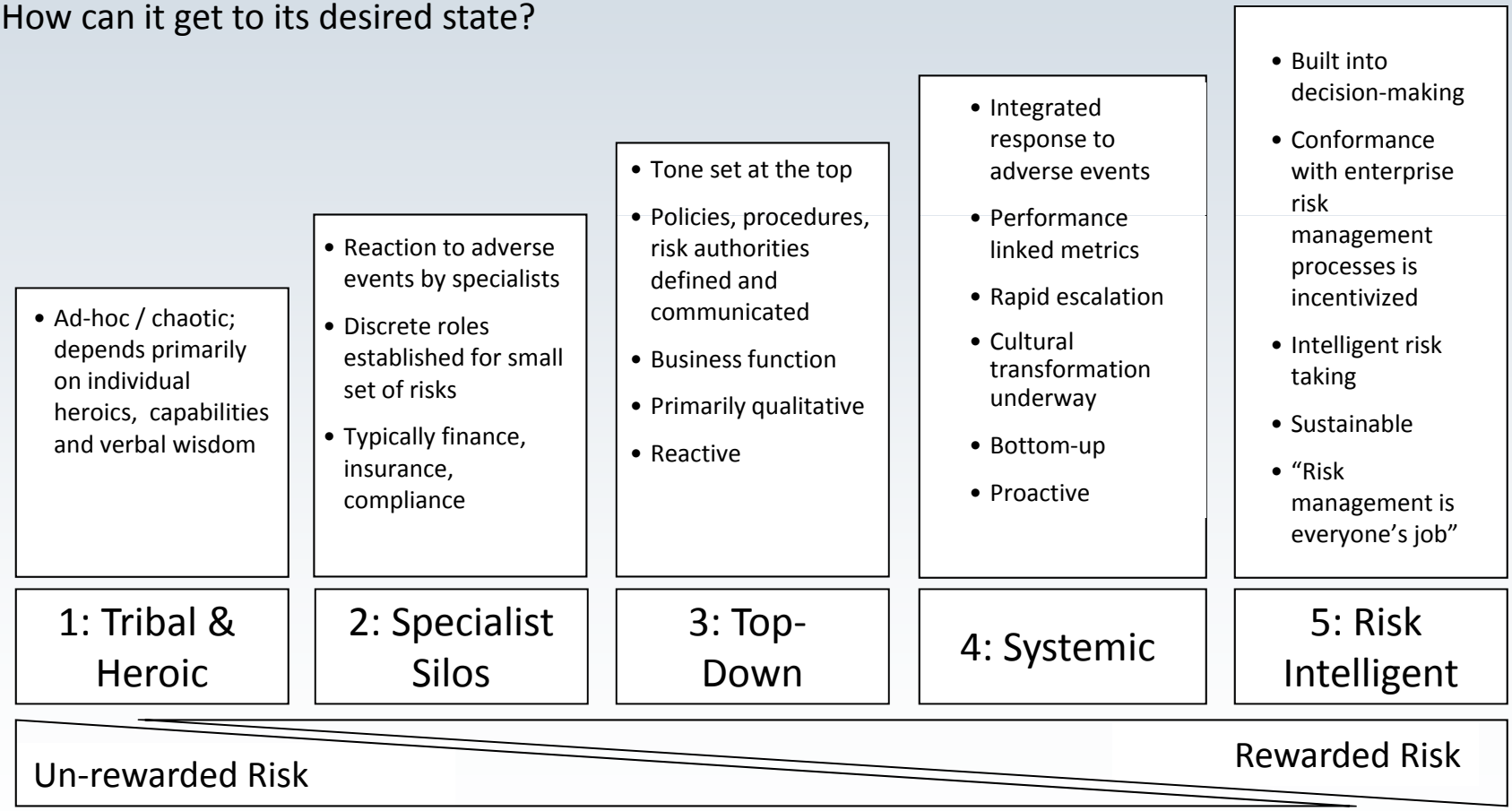
How Are Organizations Implementing?

Based on a GAIN Benchmark Study (IIA), the Status of ERM integration efforts are as follows:

ERM Specific Initiatives	Designed and/or Implemented
Periodic enterprise risk assessments performed	52%
Risks aggregated at the corporate level	49%
Enterprise-wide established policies and risk committees	30%
Risk management integrated into business initiatives	30%
Enterprise risk dashboard	30%
Risk training and knowledge sharing programs	26%
Enterprise wide risk tolerance levels and risk limits consistent	20%
Risk tolerances linked to strategic objectives	12%

A Model for Evaluating Risk Management Capability

1. How capable is your Organization today to manage its risk profile?
2. How capable does it need to be?
3. How can it get to its desired state?



CliftonLarsonAllen

IMA Maturity Model for ERM

Phase I: Building a Foundation for Business Risk Management	Phase II: Segment-Level Business Risk Management	Phase III: Enterprise-Level Business Risk Management
Phase Objectives • Build executive-level support • Strengthen core team and operating model • Align expectations through a risk management commitment process • Develop segment-level risk management commitments	• Execution of a consistent risk management approach across all segments • Engagement in specific areas to help the business remediate significant risk issues and fulfill their segment risk management commitment • Segment-level personnel at appropriate levels engaged in the risk management process • Demonstrating the tangible value of a disciplined risk management process within each segment	• Evolve to an Enterprise Risk Commitment and accountability model by "connecting" the Segment Risk Commitments to consider cross-segment risk issues and interdependencies • Enhance coordination and integration among Segment Business Risk Services (BRS) teams to help the enterprise remediate significant risk issues and fulfill the Enterprise Risk Commitment • Deepen risk management focus on potential risk issues applicable to all business segments • Enhance coordination with other components of the Enterprise Risk Management Operating Model that focus on specific areas of risk exposure

Stage Objectives:

Stage 1: Awareness	Stage 2: Capability	Stage 3: Alignment	Stage 4: Engagement	Stage 5: Value	Stage 6: Operationalize	Stage 7: Collaborate	Stage 8: Coordinate	Stage 9: Integrate
Build Risk Management Vision, Strategy & Awareness	Build Initial Risk Management Foundation of Structure, Resources and Operating Model	Align Expectations through a Risk Management Commitment	Engagement in Specific Risk Issues to Help Fulfill the Risk Management Commitment	Demonstrating Tangible Value from a Disciplined Risk Management Process	Segment-Level Personnel at All Levels Fully-Engaged in and Operationalizing the Risk Management Process	**Enhance BRM Collaboration Across Other Segment Teams to Consider Cross-Segment Risk Issues and Interdependences**	Enhance BRM Coordination with Other Areas	BRM is Fully-Integrated with Business Planning, Performance Management, Quality and Other Key Management Processes

PART THREE OF FOUR

Developing an action plan for implementation

(the "tactical")

CliftonLarsonAllen

DISTINCT ERM ROADS AVAILABLE

Option 1 - Implementing a Full-Scale ERM Model

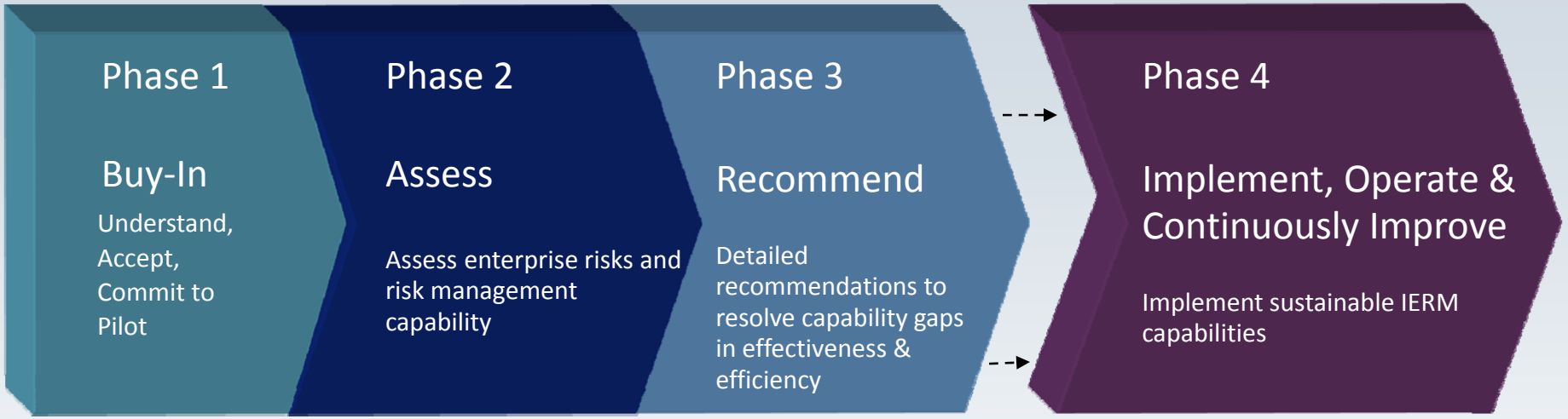
- Implementing a full program as further described and documented through facilitated sessions, documentation and meetings

Option 2 - Implementing an ERM-Lite Model

- Implementing a top-level assessment using surveys, interview questionaires and conference calls

Option 3 - A hybrid *(customize your own model including "the best of both" for your organization*

A Typical Framework for Implementation



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

- ✓ Pilot test
- ✓ Set risk appetite and 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 & set priorities

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

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

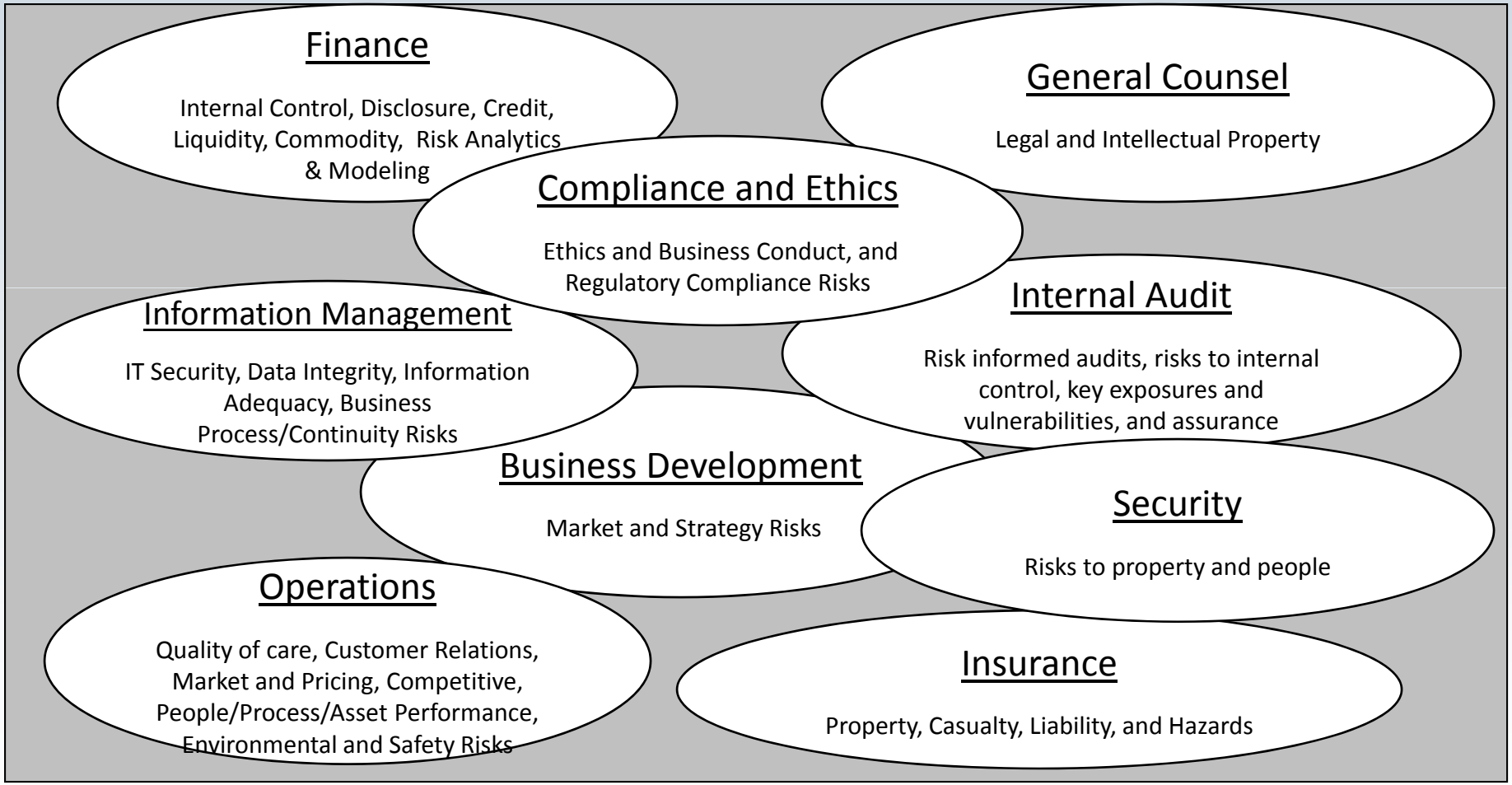
Questions Process Owners Should be Able to Answer

For each of your risks:

- How does this risk relate to achieving your objectives?
- What is the organization's appetite for risk or what is its tolerance for deviating from expected results?
- What is your state of preparedness?
- How do you know? How confident are you?
- What are the risks where you really need to improve our risk management?
- Which of these risks are most likely to occur and why?
- What is your overall risk mitigation plan?
- How will you monitor the effectiveness of the plan?
- Are there other risks on or over the horizon that you need to start to prepare for now?

Most organizations rely on multiple sources for answers

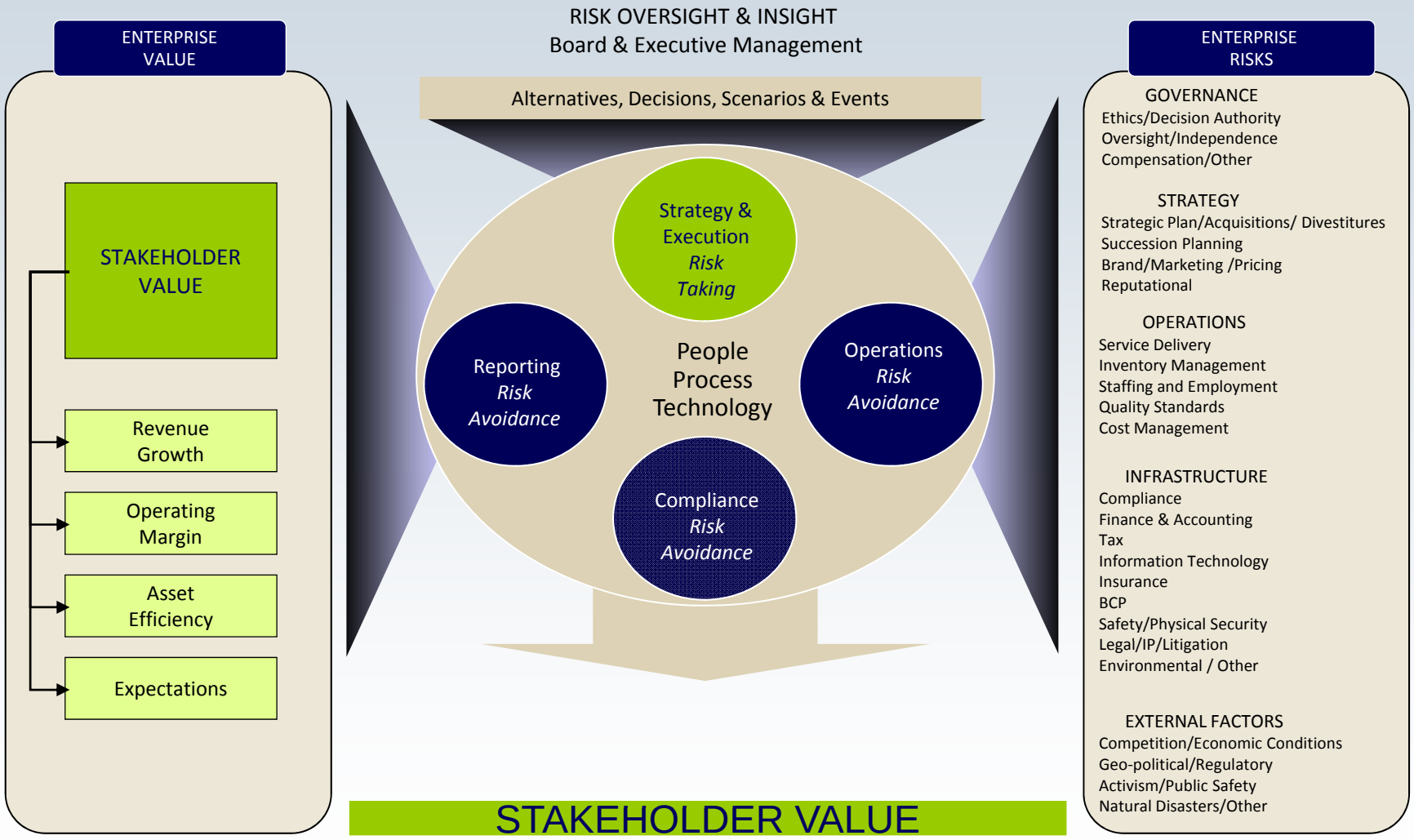
However, risk oversight and an integrated approach is usually lacking



ERM provides a means to better understand, communicate and respond to the risk knowledge that exists in the organization

CliftonLarsonAllen

An Integrated ERM Approach



Rewarded risk can *drive* value. Unrewarded risk can *destroy* value.

CliftonLarsonAllen

Top 10 Steps of Implementing an ERM Program

1. **Obtain Executive Team and Board of Directors Buy-In and Support**
   - Hold a meeting to discuss ERM and the Organization's need to implement
   - Assign risk governance oversight responsibility
   - Assign a Chief Risk Officer – A "champion" within the Organization
   - Communicate requirements of ERM

2. **Define the elements of your ERM program in simple, clearly defined terms**
   - Remember, risk is neutral. It can be either positive (an opportunity) or negative (an issue).
   - Risk – The possibility of an event occuring that would negatively affect the achievements of objectives.
   - Risk Tolerance – Levels of risk clearly established in an Organization's internal environment.
   - Opportunity – Attempting to increase the Organization's value by taking on risk.
   - Risk Appetite – The level of risk that an Organization is willing to take on as part of its process to set objectives.

Illustrative ERM Roles & Responsibilities

Party	Responsibility	Monthly or as Needed	Quarterly	Semi-annually
Board / Audit Committee	**Establish risk appetite; Review enterprise risks**			**Review all relevant risk**
Executive Management (select group or working committee)	**Set policy, prioritize and allocate resources for overall corporate risks**	**Review risks and allocate resources** **Provide guidance for significant new risks**	**Review risks and allocate resources**	**Review risks and allocate resources; report updates to Board / Audit Committee**
ERM Team (PMO, Council, Committee, etc.)	**Manage process, tools and data**	**Coordinate and assist**	**Assist with reporting and review**	**Assist with reporting and review** **Monitor program effectiveness**
Division A Management Team	**Identify, assess & monitor risks relevant to division**	**Report / escalate significant new risks**	**Report all relevant risk**	**Review risks with Executive Management**
Division B Management Team	**Identify, assess & monitor risks relevant to division**	**Report / escalate significant new risks**	**Report all relevant risk**	**Review risks with Executive Management**
Division C Management Team	**Identify, assess & monitor risks relevant to division**	**Report / escalate significant new risks**	**Report all relevant risk**	**Review risks with Executive Management**
Corporate Management Team	**Identify, assess & monitor risks relevant to corporate functions**	**Report / escalate significant new risks**	**Report all relevant risk**	**Review risks with Executive Management**

Top 10 Steps of Implementing an ERM Program

3. Determine your Organization's Risk Tolerance

- How much risk is this organization willing to accept? High? Low? Moderate?
- How does your strategic plan fit in?

4. Determine Materiality ranges at the entity level and by business units, as applicable

For Example:

Measure	Low-End of Range	High-End of Range
Revenue	1%	5%
Assets	0.25%	0.50%
Equity	1%	5%

Top 10 Steps of Implementing an ERM Program

5. Identify a Risk Inventory Library with the help of a facilitated session

6. Determine the probability of significant risks occuring and their magnitude

7. Determine how risks will be managed

8. Develop a detailed Activity-level Risk Assessment

9. Confirm and develop the level of reporting needed by Executive Management and the Board of Directors

10. Establish communication protocal & management of the on-going ERM process

Overall Risk Profile – Library Index

Strategic Risk		Operational & Process Risk		Financial/ Reporting Risk	Compliance
Business Model	Innovation	Customer Satisfaction	Environmental	Interest Rate	Regulatory Reporting
Board Governance	Capital Availability	Human Resources	Health and Safety	Currency	Migrant Labor
Human Resource	Political	Product Development	Human Resources	Permanent Equity	International Trade Laws
Competition	Legal	Efficiency	Outsourcing	Commodity	Product Safety
Industry Consolidations	Industry	Capacity	Performance Incentives	Liquidity	Anti-Trust
Energy & Material Costs	Ethics	Scalability	Information Technology Integrity	Concentration Customer/ Credit/Other	
Budget and Planning	Succession Planning	Commodity Contracting	Information Technology Availability	Collateral	
Product Availability	Image and Branding	Partnering	Information Technology - Infrastructure	Cash Flow	
Contract Commitment	Reputational	Product/Service Failure	Fraud & Illegal Acts	Opportunity Cost	
Investment Valuation	Catastrophic Loss	Business Interruption		Internal Control Environment	
Resource Availability				Pensions & Health/Welfare	
				Financial Reporting	

Major Types of IT Risk and IT Risk Areas

IT Computing Environment

- Hardware, Software
- System interfaces, Databases
- System and data criticality (system's importance to the organization) & sensitivity
- Data backup and recovery process

Logical Access

- Password Administration
- Direct and Physical access to data, data centers/facilities/equipment
- Lack of segregation of duties

Network Security and Availability

- System security policies & architecture

Operational Environment of IT systems

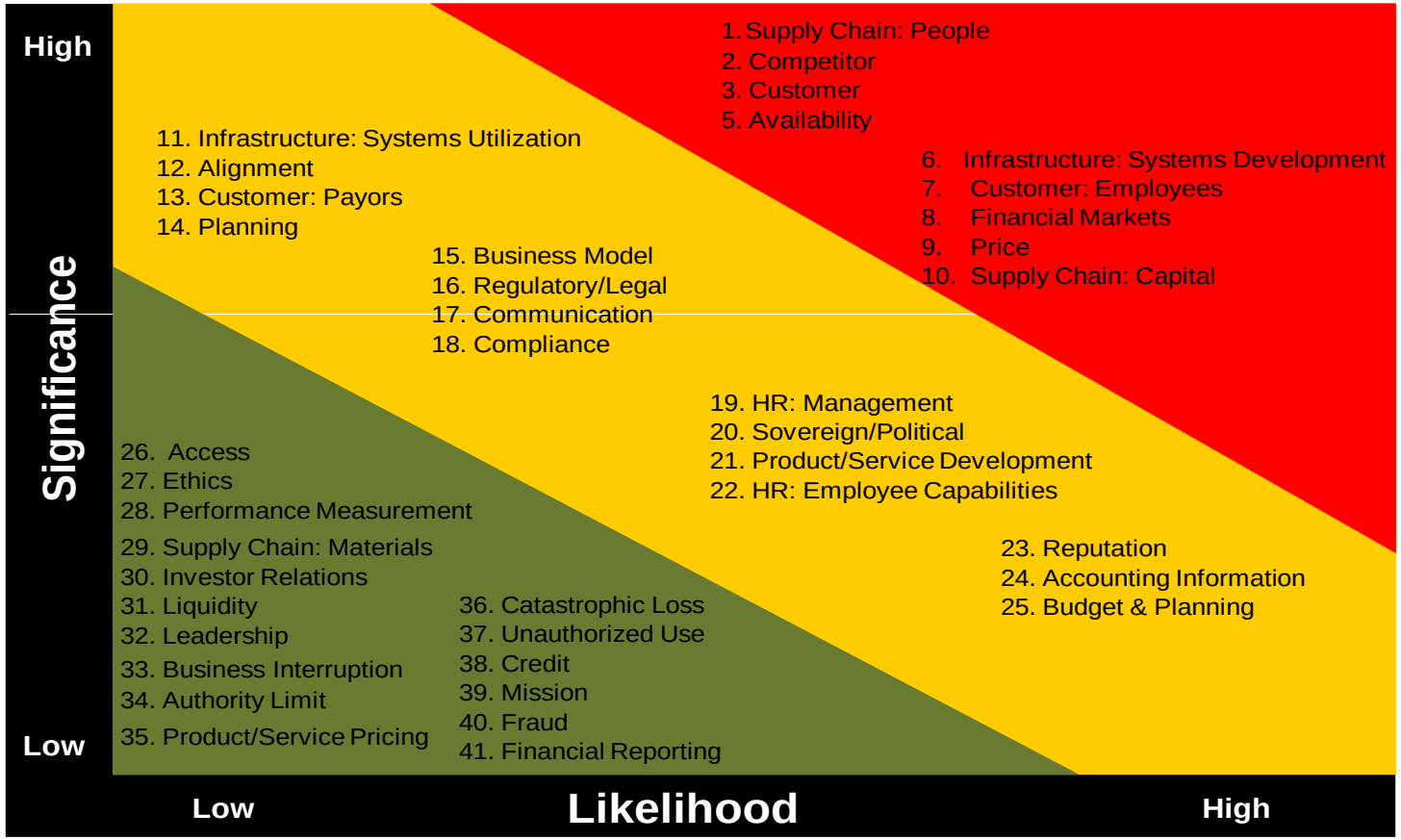
- Functional requirements of IT system
- Users of the IT system
- Management of data changes

Risk Rankings - Framework

- We recommend utilizing a numeric risk ranking model as part of the risk assessment

- Depending on the potential risk universe, to further delineate and differentiate risks, we recommend using the following:
  - Likelihood
  - Impact
  - Tolerance
  - Pervasiveness

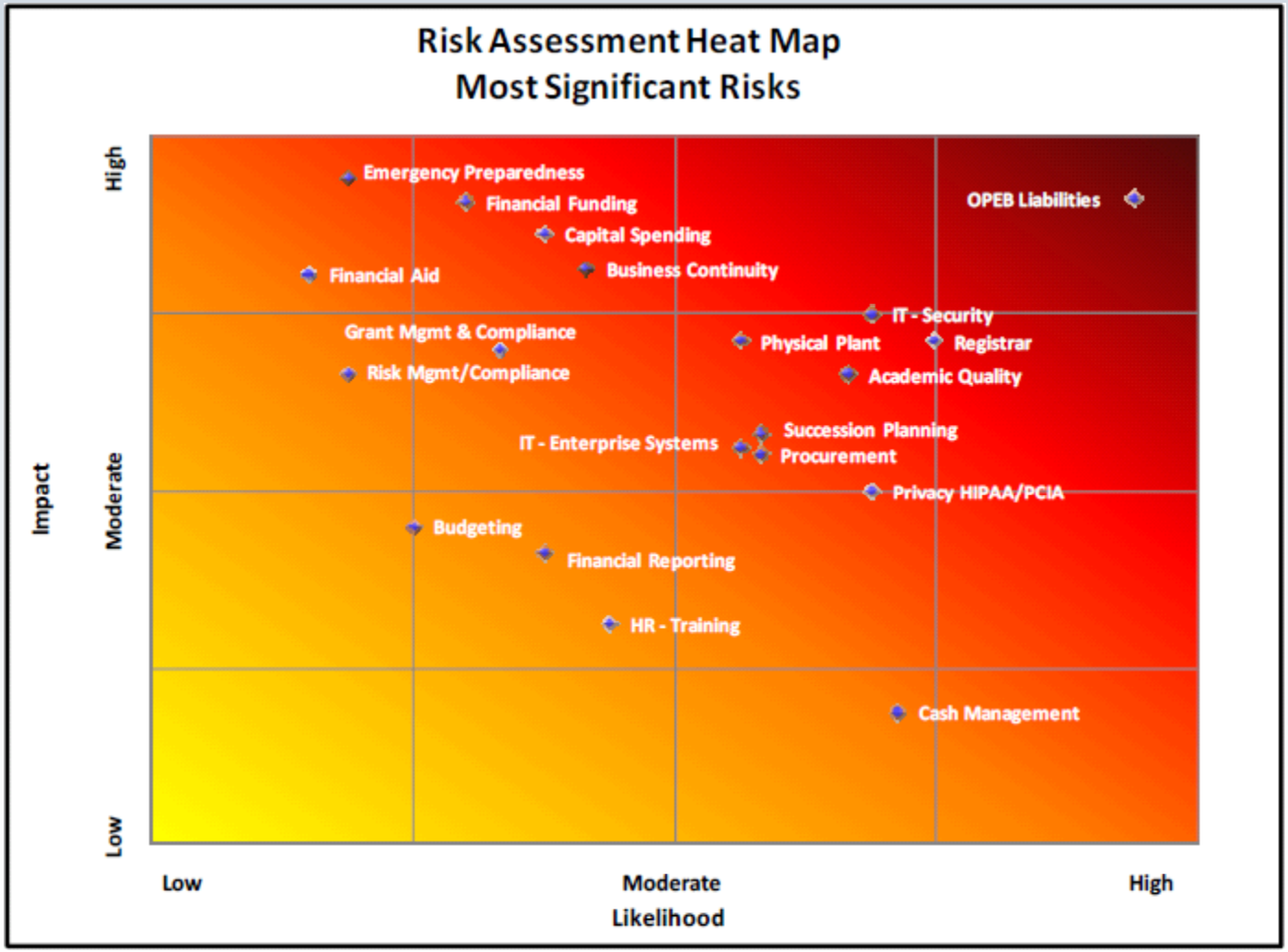
Prioritized Risk Profile



High Moderate Low

CliftonLarsonAllen

Results – Sample Heat Map



CliftonLarsonAllen

Critical Success Factors

- Gain Board / senior executive commitment and involvement
- Establish management accountability and responsibilities
- Demonstrate tangible results and link to value objectives
- Build the process into the way the enterprise does business
- Obtain supporting charter, policies, and procedures
- Focus on the cultural/change management process
- Monitor and continuously improve

PART FOUR OF FOUR

Questions and Answers