Effective and Impactful Risk Assessments

CliftonLarsonAllen

cliftonlarsonallen.com

Discussion Objectives

1. Identify factors driving the need for Risk Assessment and Risk Management functions and processes

2. Discuss processes for identifying, assessing and prioritizing risks, and how to align this with an internal audit plan and corporate objectives

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

Factors Driving Risk Management:

Why Do You Do It?

What is Risk Management and Risk Assessment?

Enterprise risk management is a process, effected by the entity's board of directors, management, and other personnel, applied in strategy-setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within the risk appetite, to provide reasonable assurance regarding the achievement of objectives.

- COSO Enterprise Risk Management – Integrated Framework 2004

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

What are Working Definitions??

Organizational definitions of Enterprise Risk Management (ERM) and ERA can vary. At its basic core – risk assessment (as a foundation/precursor for risk management), involves having a better understanding of the risks your organization faces, and having a sustainable and repeatable process to successfully identify, prioritize, mitigate and monitor them.

By extension, Risk Management can be applied not just on an enterprise level, but can be deployed by business unit (Agency, Bureau, IT, Accounting, Compliance, etc.), by functional area (Operations, Strategy, Finance, etc.), or by other means (practice area, facilities, etc.). The key is understanding what risk and/or risk assessment and monitoring related processes and functions exist, and at which levels, within your organization.

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 Many Organizations Are Asking

- What is our appetite for risk and what is our tolerance for deviating from expected results?
- What risks should we be focusing on? Do we know what our true top risks are?
- Once we know what the risks are, how prepared are we to address them?
- How well are we doing with the risks we are focusing on?
- Do we have a sustainable process to make risk assessment more than a one time event?
- 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??***

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.

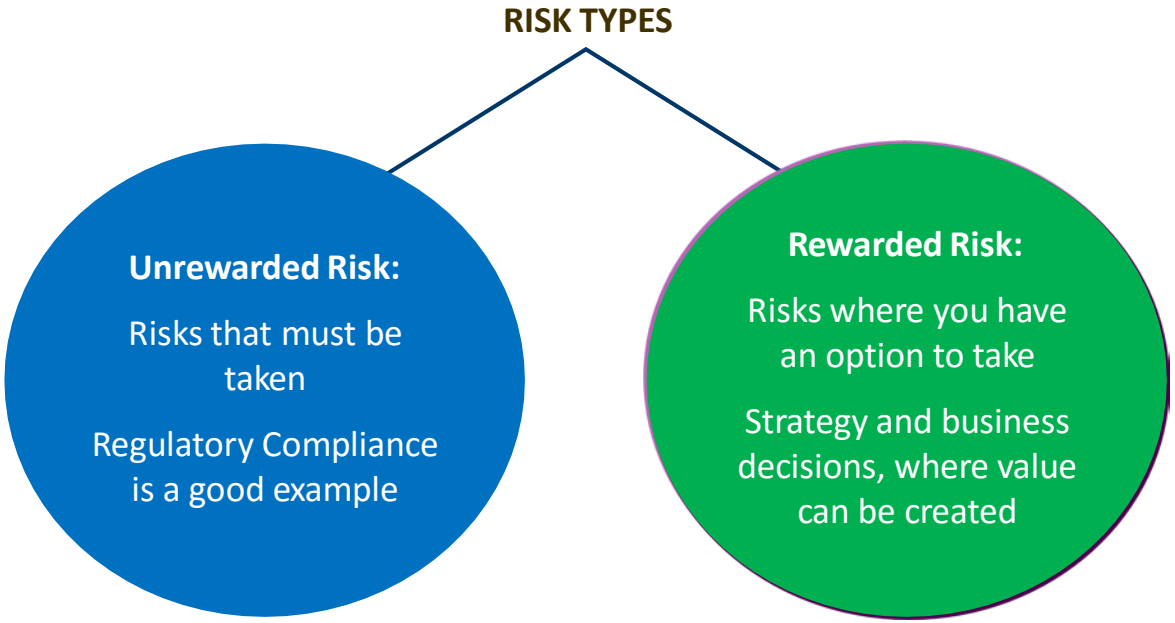
- Risk Tolerance – *acceptable level of uncertainty or variability of outcomes related to performance measures or specific objectives of the organization*
- Risk Appetite – *broad description of the level/amount of risk an organization is willing to take as part of its goals/strategy*
- Definitions vary – 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

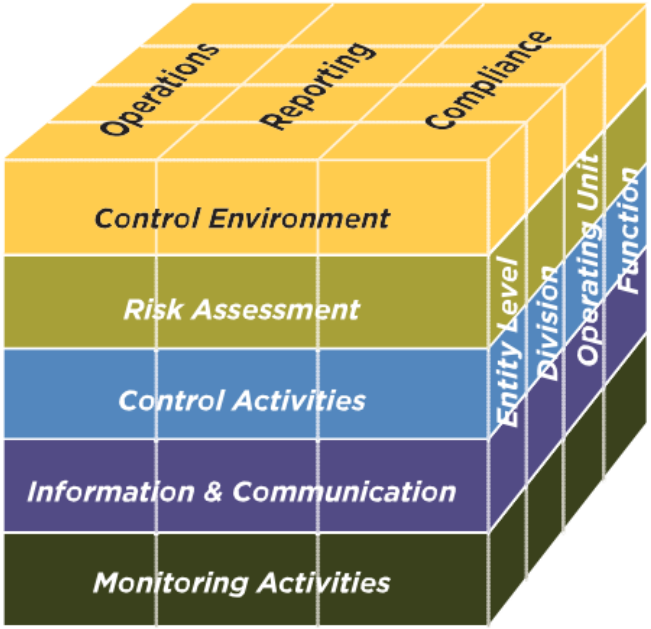


Fail to manage the Unrewarded Risks and negative implications ensue

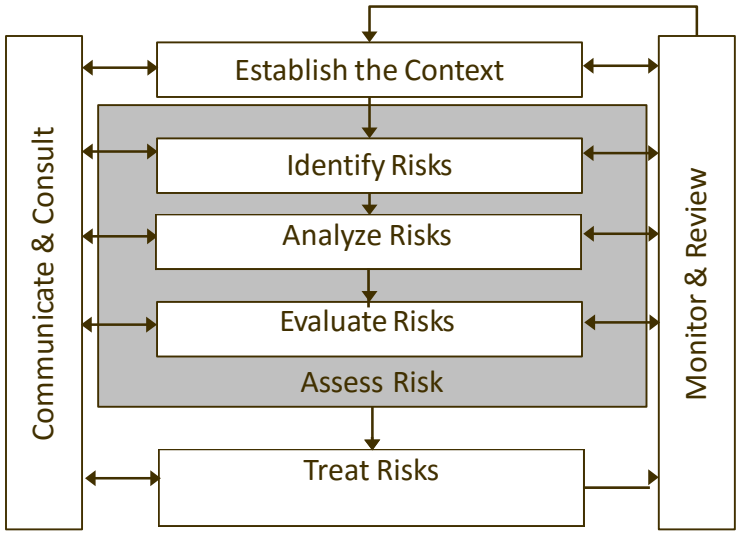
Fail to take the right amount of Rewarded Risks and you miss opportunities

Two Popular Risk Frameworks

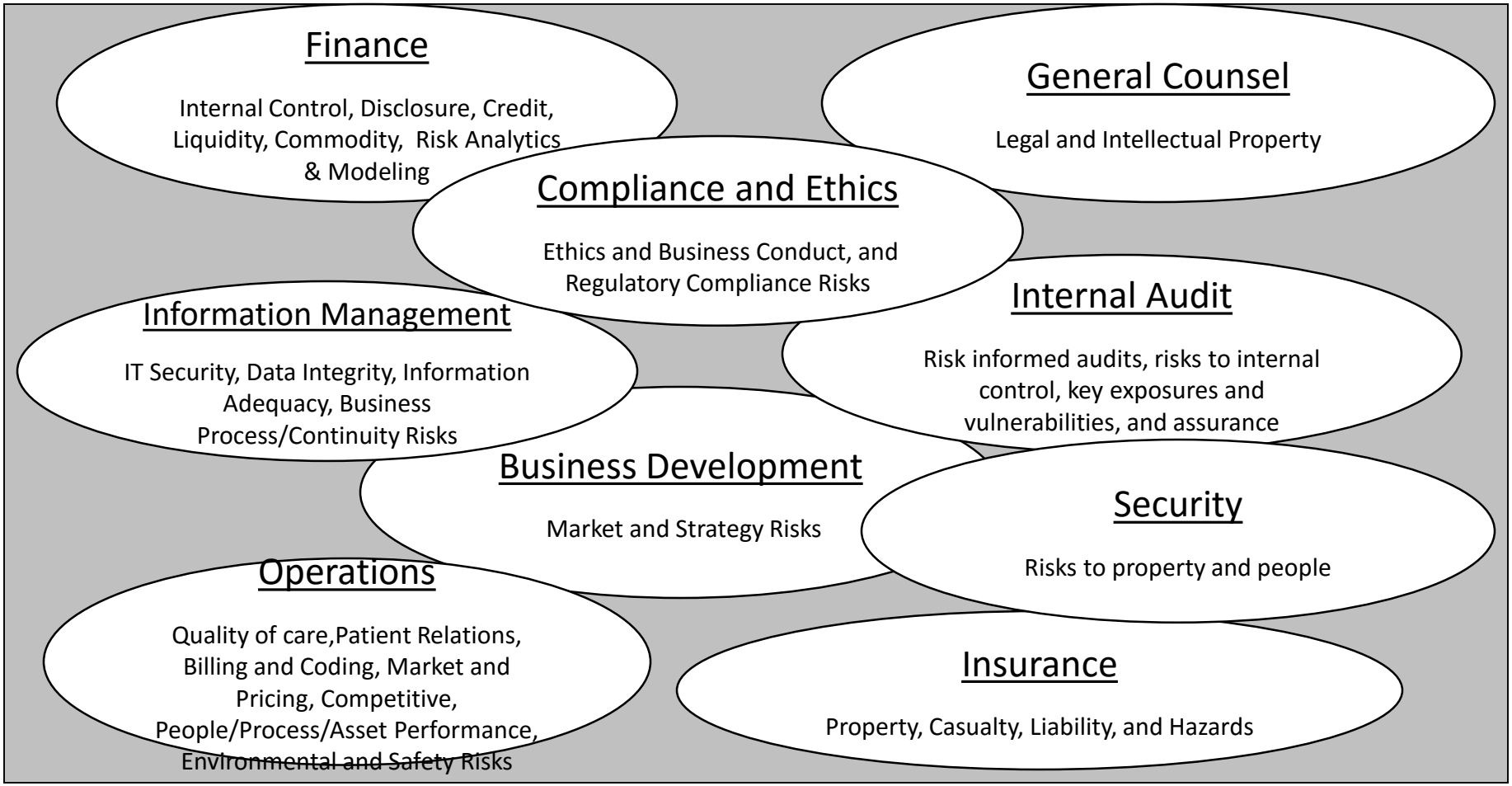
COSO integrated framework - 2013



AS/NZ - ISO 31000:2009

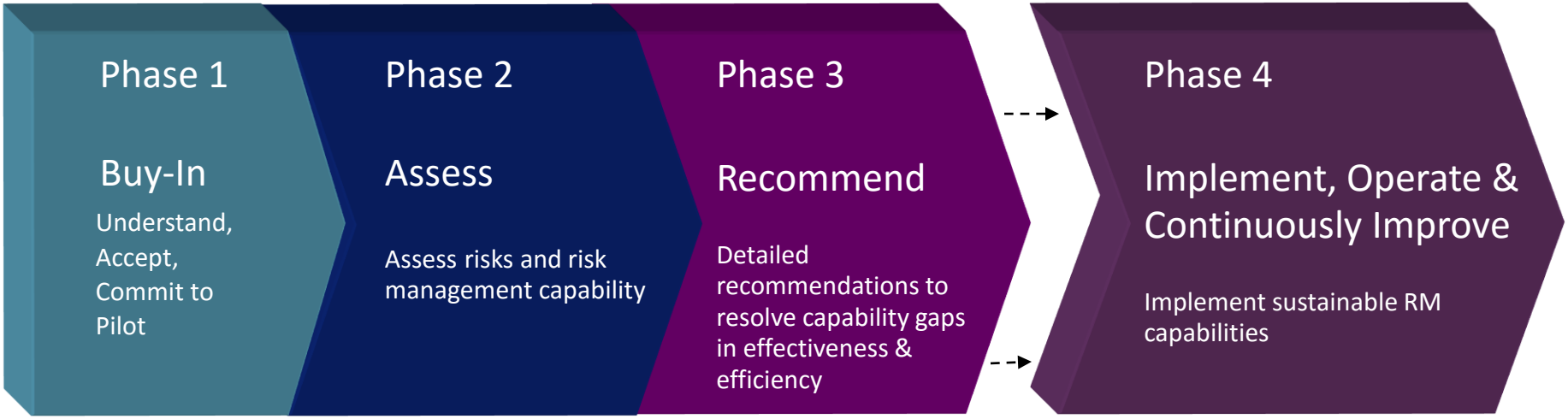


Goals of Risk Management & Risk Assessment



Challenge is how to align and integrate all these various groups; and how to get Internal Audit to align and "overlap" with each area

Progression to Integrate Risk Management



- ✓ Value Proposition
- ✓ Clarify RM needs & expectations
- ✓ **Executive awareness and commitment**
- ✓ **Agree on scope, criteria, process**
- ✓ Establish RM 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**

Leading Practices: Audit Planning

How To Integrate Risk Management Effectively for Audit Planning?

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.

Example of a Risk Report – &/Or Audit Monitoring

Risk Description	Risk Direction	Risk Response Status	Risk Owner	Status of Additional Risk Management Activities Initiated
Failure to comply with Federal regulatory standards	→		Mr. Avoid	• Performing review of last 12 months of adverse compliance • Developing action plans for key trend areas identified from the review
Inaccurate billing for services	↘		Ms. Accept	• Assess customer concerns • Measure customer satisfaction
Insufficient business continuity planning	→		Mr. Reduce	• A project has been initiated to develop appropriate business continuity plans for all major operations and facilities.
Inadequate IT backup and disaster recovery processes	↗		Ms. Transfer	• Key steps have been completed to improve IT BCM: consolidated and improved the data center, documented processes, and retrained personnel.

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

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?

Thank you!

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