Effective Risk Assessment & Control Analysis

Ryan Dooley
Matt Rever
Jim Kreiser

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.

Learning Objectives

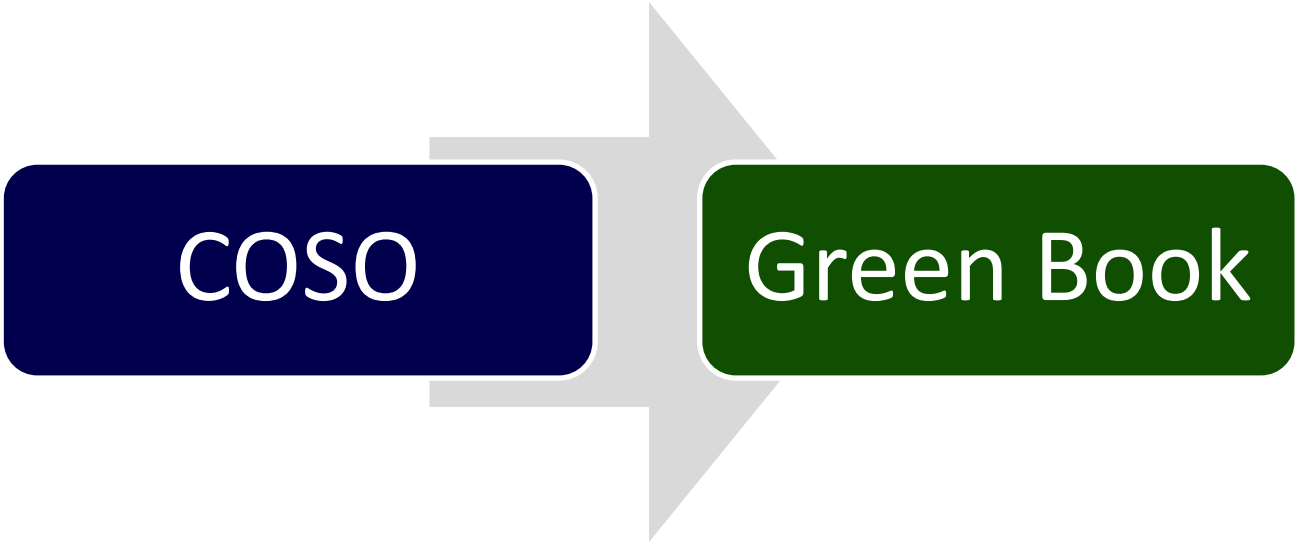
At the end of the session, you will be able to:

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

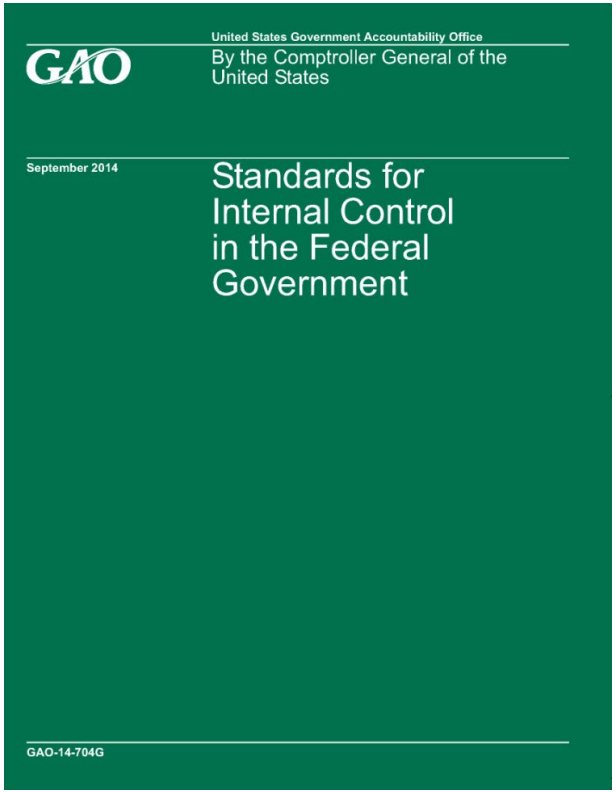
Factors Driving Risk Management

Why do you do it?

From COSO to Green Book: Harmonization



Green Book: Standards for Internal Control in the Federal Government



- Consists of 2 sections
  - Overview
  - Standards
- Establishes
  - Definition of internal control
  - Categories of objectives
  - Components and principles of internal control
  - Requirement for effectiveness

Standards for Internal Control in the Federal Government “The Green Book”

- We have internal controls to help an entity to run its operations efficiently and effectively, report reliable information about its operations, and comply with applicable laws and regulations.

- The “Green Book” sets the standards for an effective internal control system for federal agencies.

- The objective of Pennsylvania Management Directive 325.12 was to adopt and implement the internal control framework outlined in the “Green Book”.

What is Risk Management and Risk Assessment?

Enterprise risk management (ERM) 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

ERM is related to internal controls but it also includes the following concepts as preconditions of internal control:

- Risk Appetite
- Tolerance
- Strategy
- Business Objectives

Benefits of Risk Assessments

- 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
- 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

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

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

What types of risk are organizations like you focusing on?

- Many organizations are realizing that they need to focus on the full spectrum of risk categories to ensure that they have identified their true top risks, and that they are focusing on the right things.
- Risks are specific to the particular government or non-profit organizations but in addition to traditional risk categories such as finance, organizations may identify risks in areas such as:
  - Legislative and Regulatory change
  - Economic Environment
  - Vendor Management
  - Human Capital Management
  - Affiliated Organizations
  - Business Continuity
  - Fraud
  - Cyber Infrastructure
  - Social Media
  - Federal Regulatory Compliance
  - State Regulatory Compliance
  - Safety and Security
  - Reputation management

Discussion Question

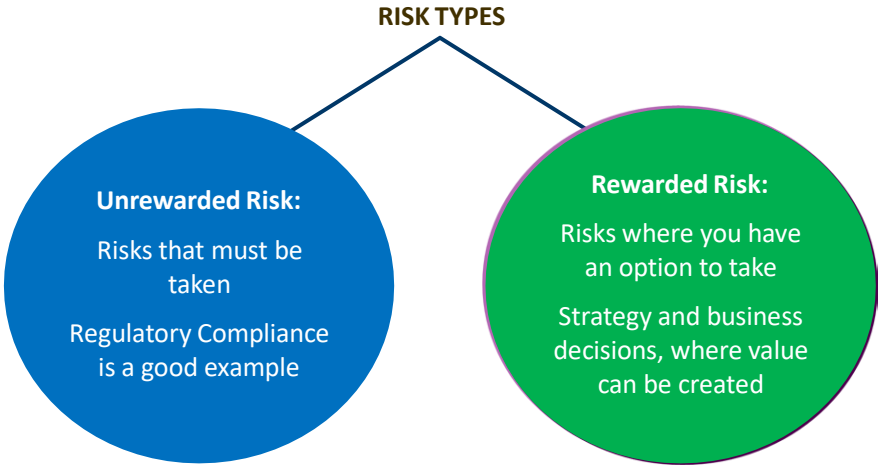
Last summer, the town of South Park was the victim of a Ransomware attack, where employee data was held in an encrypted format, preventing the town from accessing it. The town had to pay $2 million to have the encrypted malware lifted. The root cause of the attack was from an employee downloading a file from a malicious email. The town has implemented a new policy since the attack to have employees complete security awareness training on a quarterly basis.

Let’s discuss some factors driving the need for risk management?

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 ERM framework – 2013**
- **Risk Management Objectives**
  - Strategic
  - Operations
  - Reporting
  - Compliance
- **Risk Domains**
  - Internal Environment
  - Objective Setting
  - Event Identification
  - Risk Assessment
  - Risk Response
  - Control Activities
  - Information and Communication
  - Monitoring

- **AS/NZ - ISO 31000:2009**
- **More fluid approach, less structured**
- **Processes:**
  - Establish the context
  - Identify Risks (assess risk)
  - Analyze Risks (assess risk)
  - Evaluate Risks (assess risk)
  - Treat Risks
  - Communicate and Consult (continuous)
  - Monitor and Review (continuous)

Evaluating Risk Management Capacity

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

Framework for Assessing Risk and Organizing Risk Response

The risk assessment process facilitates the identification of risks by rating the **Impact**, **Vulnerability** and **Speed of Onset,** or more commonly called **likelihood**.

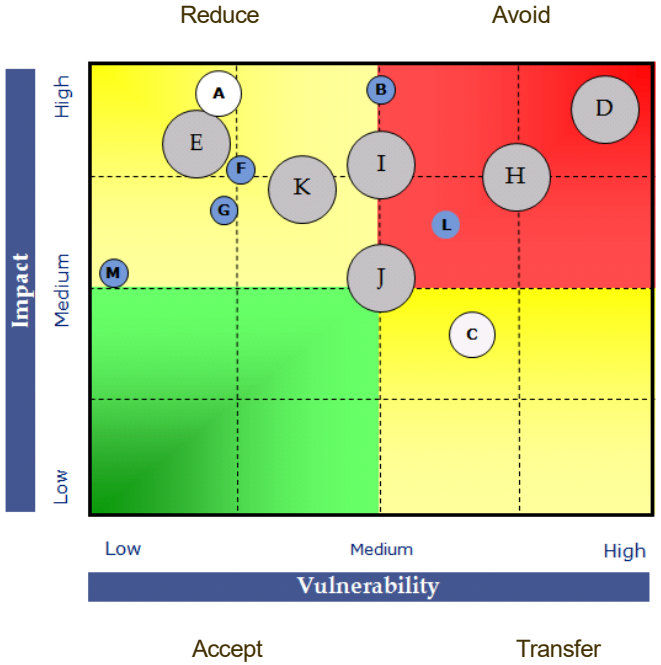
The overall types of impact of the risk can be based on multiple impacts including:

- Financial Reputation Legal/Regulatory
- Customers Employees Operations

The overall vulnerability of the risk can be based on factors such as:

- Existing controls and mitigation efforts Risk management capability
- Prior risk experience

Speed of Onset is based on how quickly the risk could occur



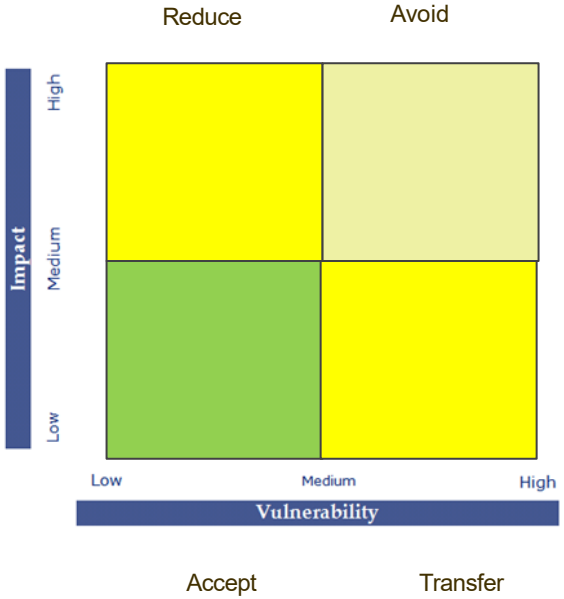
Polling Question

Risk Response Exercise

For each of the risk example below, evaluate

1) The impact level – low, medium, or high
2) The vulnerability / likelihood level – low, medium, or high
3) Risk Response – Accept, Reduce, Transfer, Avoid

	Risk Example
A	Environmental Safeguards – Server room is maintained onsite in a location where earthquakes are fairly common. The last earthquake occurred 2 years ago and destroyed a server rack that caused the primary financial system to go down.
B	
C	
D	



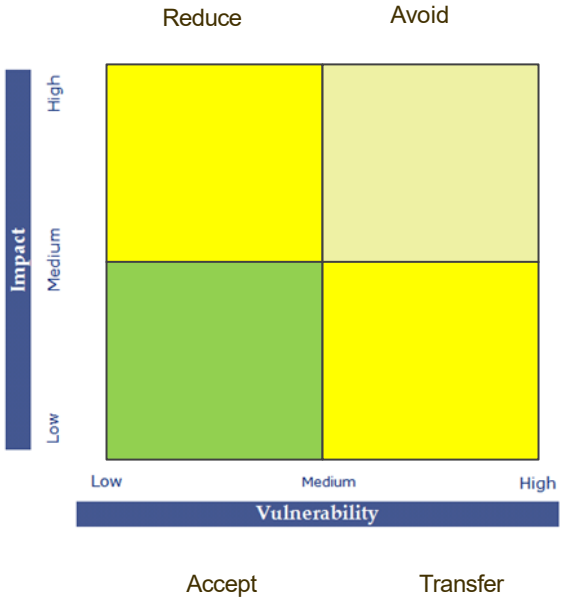
Polling Question

Risk Response Exercise

For each of the risk example below, evaluate

1) The impact level – low, medium, or high
2) The vulnerability / likelihood level – low, medium, or high
3) Risk Response – Accept, Reduce, Transfer, Avoid

	Risk Example
A	
B	Customer Service Process – Multiple customer service reps have not received proper training in following up with customers to measure their customer satisfaction rating.
C	
D	



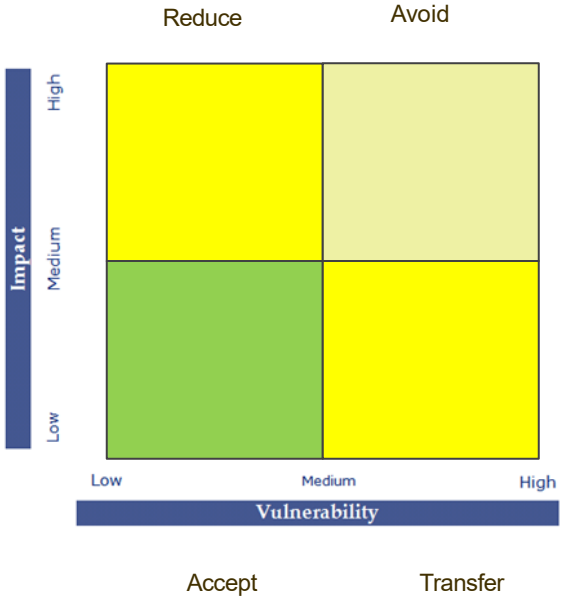
Polling Question

Risk Response Exercise

For each of the risk example below, evaluate

1) The impact level – low, medium, or high
2) The vulnerability / likelihood level – low, medium, or high
3) Risk Response – Accept, Reduce, Transfer, Avoid

	Risk Example
A	
B	
C	Payroll Process – Five (5) individuals are in charge of payroll processing in an organization. The most senior individual is scheduled to retire at the start of the summer.
D	



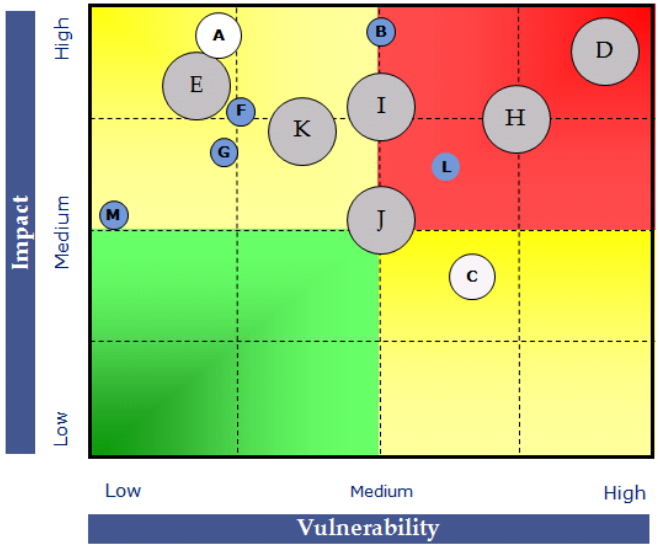
Leading Practices for Risk Assessments

How to integrate risk management effectively for audit planning

WEALTH ADVISORY | OUTSOURCING
AUDIT, TAX, AND CONSULTING

Shortcoming with Heat Map / Likelihood Model

- Lack of alignment with goals
- 80% of all major value losses are high impact / low likelihood
- Human bias
- Typically focuses on single events rather than a series of events or domino effect



Another Way to Think/Conceptualize the Risk Assessment and Planning

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.

The Key is to utilize an approach and framework that works for the organization and can integrate with the organizational goals and objectives.

Risk Rankings?

- 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 RA 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

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

Operations Planning

- How should operations react to a risk assessment:
  - Consider the risks and impacts.
  - What controls are in place? Can they be automated?
  - Are new controls needed?
  - Are good written procedures in place and communicated?
  - Could this affect how you prioritize projects and resources?

Consider the risks and impacts

- Risk Mitigation is the process of planning for disasters and having a way to lessen negative impacts.
  - Accept Risk
  - Avoid Risk
  - Transfer Risk
  - Reduce Risk

What controls are in place? Can they be automated or semi-automated?

- Control Components
  - The subject matter to which the control is applied
  - The party responsible for performing the control
  - The nature of the activity performed, including sources of information used in performing the control
  - The frequency with which the control is performed or the timing of its occurrence
- Automated
  - Function of the control is systematically performed
- Semi-Automated
  - Function of the control is dependent on system generated process or report, but require human interaction to complete

Are new controls needed?

- Control Gaps
  - When a control does not exist, does not effectively mitigate a risk or is not operating effectively.
- Control Design
  - Address the risk in question
    - Documentation
    - Authorization
    - Approval
    - Reconciliation
    - Segregation of duties
    - Access Security
    - Supervision
    - Reporting

Are good written procedures in place and communicated?

- Identify any gaps
- Are policies and procedures reviewed and approved by appropriate personnel on an annual basis?
- How are these policies and procedures furnished to staff?
- When changes are made, how are those furnished to staff?
- How is compliance with policies and procedures assessed?

Could this affect how you prioritize projects and resources?

- Your prioritization could be affected based on your assessment of risk rankings
  - Prioritize the higher risk rankings and remediation plans
  - Risk rankings can be based on high, medium, low or more granular numeric quantification method

- Which in turn, will get you to identify criteria in your prioritization of projects. Some examples of criteria used in prioritization:
  - Capacity
  - Investment (ROI)
  - Outside factors
  - Budgeted funds
  - Timing, if there are any dependencies or limitations

Questions?

Thank You

Ryan Dooley, CPA, CISA, CCSFP
Ryan.dooley@CLAconnect.com

Matt Rever, MIS, CISA
Matthew.Rever@CLAconnect.com

Jim Kreiser, CISA, CRMA, CFSA

CLAconnect.com

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING