COSO Based Risk Assessment

Internal Audit Office (IAO)

Mei Gentry

June 16, 2022

Introduction

Objectives

- Identify the objectives, components, and principles in the COSO Framework.
- Describe risk appetite and risk tolerance.
- Explain the difference between inherent risk and residual risk.
- Recognize the COSO Framework concepts of likelihood and impact in determining risk significance.
- Apply risk assessment concepts to a risk assessment scenario.

Risk Assessment

Internal controls - provide reasonable assurance that the agency will successfully achieve its objectives

Internal Audit - well positioned to interact with management assess risks holistically

COSO Framework:

- control risks to an acceptable levels and achieve the agency's objectives.
- offers practical guide for risk assessment
- link audit activities to the processes that are most critical

COSO
(Committee of Sponsoring Organizations)

5 sponsoring organizations:
American Institute of Certified Public Accountants (AICPA)
American Accounting Association (AAA)
Financial Executives International (FEI)
Institute of Internal Auditors (IIA)
Institute of Management Accountants (IMA).

COSO's goal is to provide thought leadership dealing with three interrelated subjects: enterprise risk management (ERM), internal control, and fraud deterrence.

Enterprise Risk Management — Integrated Framework (2004, 2017)

Internal Control - Integrated Framework (1992, 2013).

Fraudulent Financial Reporting: 1987-1997 studies (1999)
Fraudulent Financial Reporting: 1998-2007 studies (2010)

Internal Controls Framework

Components	Principles	No. of Points of Focus
Control Environment	1. Commitment to integrity and ethical values	4
	2. Independent board of directors oversight	4
	3. Structures, reporting lines, authorities, responsibilities	3
	4. Attract, develop and retain competent people	4
	5. People held accountable for internal control	5
Risk Assessment	6. Clear objectives specified	5
	7. Risks identified to achievement of objectives	5
	8. Potential for fraud considered	4
	9. Significant changes identified and assessed	3
Control Activities	10. Control activities selected and developed	6
	11. General IT controls selected and developed	4
	12. Controls deployed through policies and procedures	6
Information & Communication	13. Quality information obtained, generated and used	5
	14. Internal control information internally communicated	4
	15. Internal control information externally communicated	5
Monitoring Activities	16. Ongoing and/or separate evaluations conducted	7
	17. Internal control deficiencies evaluated and communicated	3

- No “one size fits all” solution for designing a risk assessment process
- COSO Framework provides practical guidance on measuring and prioritizing risks, which is the basis for the organization’s risk response.
- The goal of risk assessment is to determine how to manage risk levels within a defined threshold while preserving the organization’s ability to act on opportunities in line with its strategic goals. (costs and benefits)
- The identification and analysis of risk is performed by management.
- The key risks identified by management become the focus for internal audit to evaluate the design and effectiveness of key controls.

Risk Assessment – 4 Principles

- Principle 6: The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

- Principle 7: The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.

- Principle 8: The organization considers the potential for fraud in assessing risks to the achievement of objectives.

- Principle 9: The organization identifies and assesses changes that could significantly impact the system of internal control.

Starting with Management

Audit Risk Assessment

- Opportunity for internal auditors to collaborate with multiple levels of management to gain an understanding of how risks impact the organization's strategies
- Gain insight on the effectiveness of the organization's culture and governance.
- Dynamic (not checklist); Enterprise/aggregate (not silo)

Risk Assessment Approach

Using both approaches ensure key risks are identified and addressed.

Clear Understanding:

Risk Universe Completeness

Once internal audit knows the organization's objectives and the business processes used to achieve those objectives, they can evaluate the completeness of the key risks identified.

There are known knowns. These are things we know that we know. There are known unknowns. That is to say, there are things that we know we don't know. But there are also unknown unknowns. There are things we don't know we don't know. - Donald Rumsfeld

Does the risk you're taking align with your stated risk tolerance?

Holistic risk management and fiduciary confidence

Investment/portfolio risk

Risks associated with **excess return or alpha** need to be **optimized**, not minimized.

- Investment strategy
- Fund oversight
- Performance measurement
- Performance attribution

Enterprise legal risk

Risk characterized **strictly by risk of loss should be minimized** to the extent that it's **cost-effective** and practical.

- Compliance oversight monitoring
- Business continuity management
- Risk and control assessments
- Regulatory developments

High-tech client experience, industry-leading **financial reporting**

Minimized unauthorized activities, service interruptions, **regulatory exposure**

Operational risk

These risks include high-qualty transaction processing and adherence to regulatory guidelines.

- Vendor management
- Processing excellence
- Best-in-class reporting
- Safeguarding of assets

Source: Vanguard.

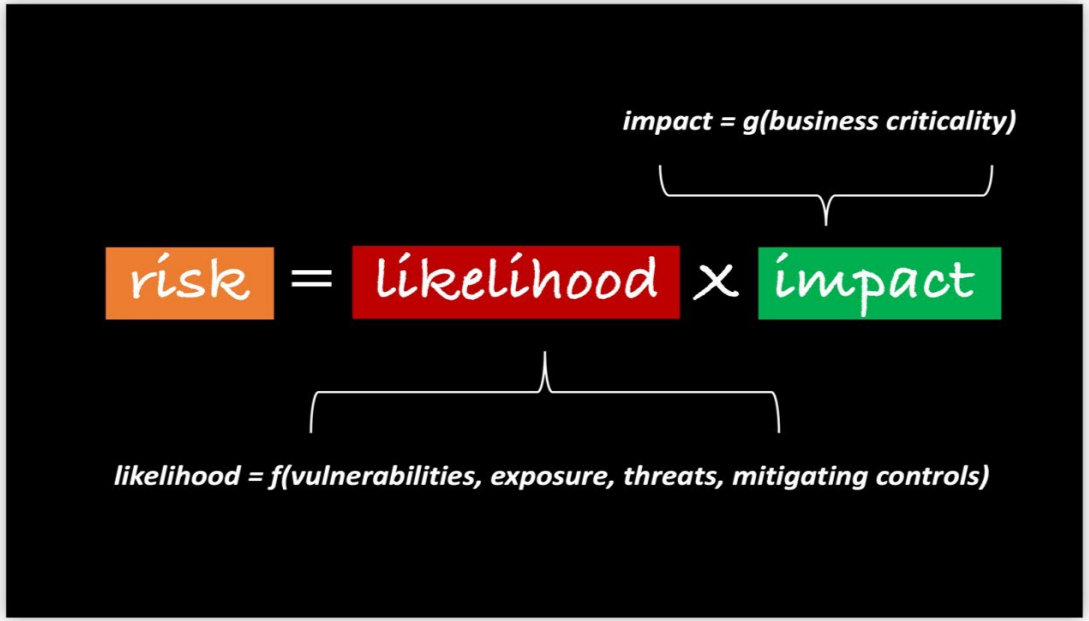
Categories of Risk

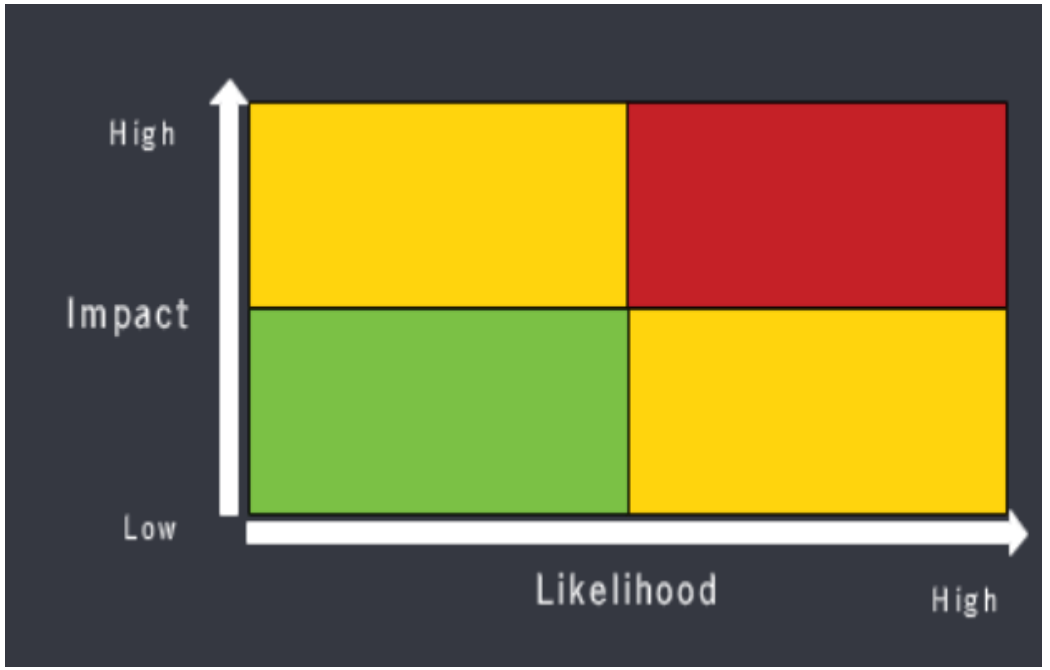
- Entity-Level Risk - Risk that affects the overall entity
- Operations Risk - Risk to an organization's internal processes, people, and systems
- Financial Risk - Risk to an organization's ability to achieve its financial goals and safeguard its assets
- Compliance Risk - Risk to an organization's ability to comply with laws, regulations, codes of conduct, and standards

Entity-Level Risks	Operational Risks	Financial Risks	Compliance Risks
Change in regulations	Supply	Available capital	Fraud
Economic turmoil	Manpower	Interest rates	Governance
Competition	Communication	Currency exchange	Ethics

The most potential to prevent the achievement of process-level objectives should be included in the audit plan

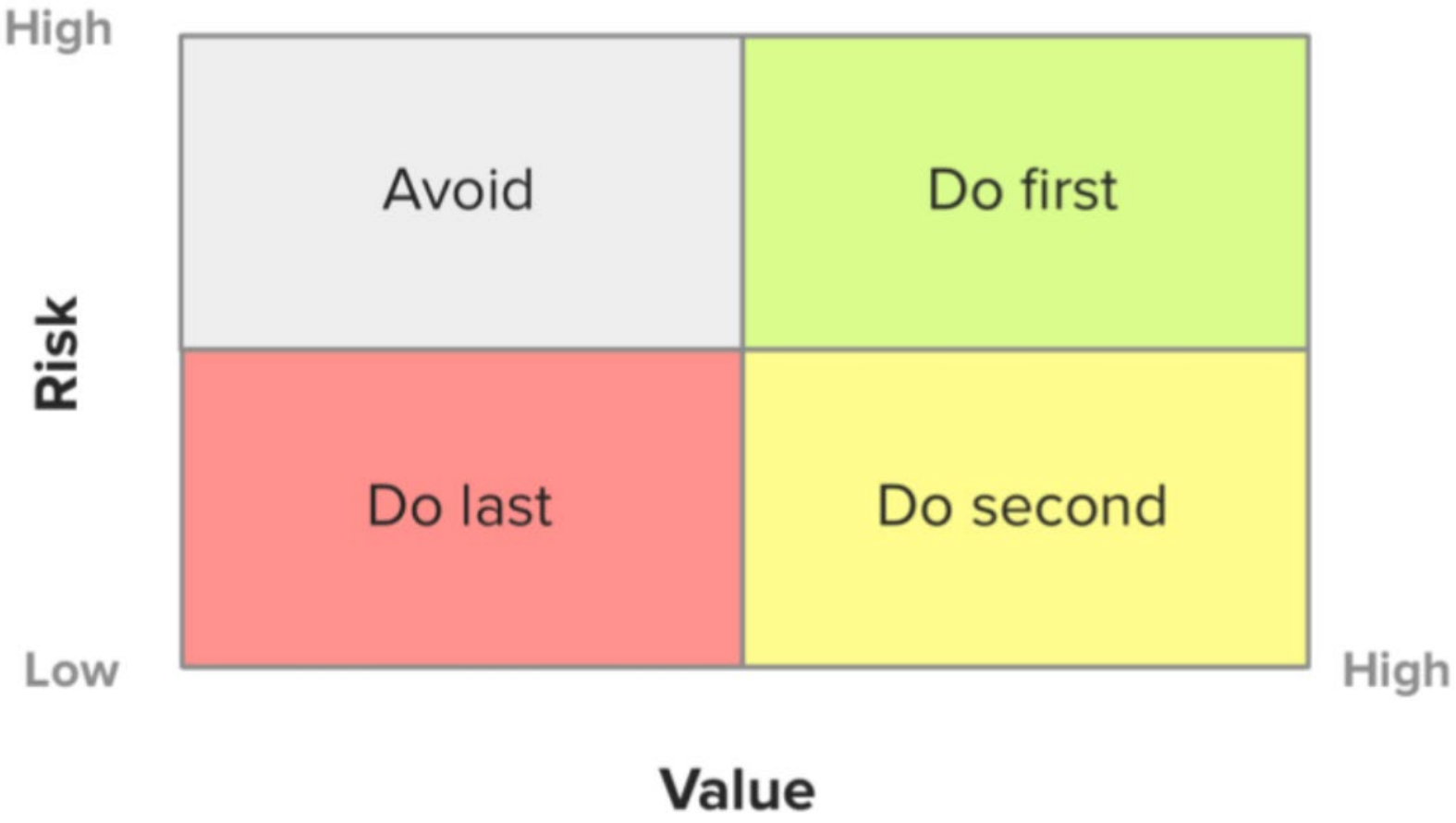
Risk Analysis Process



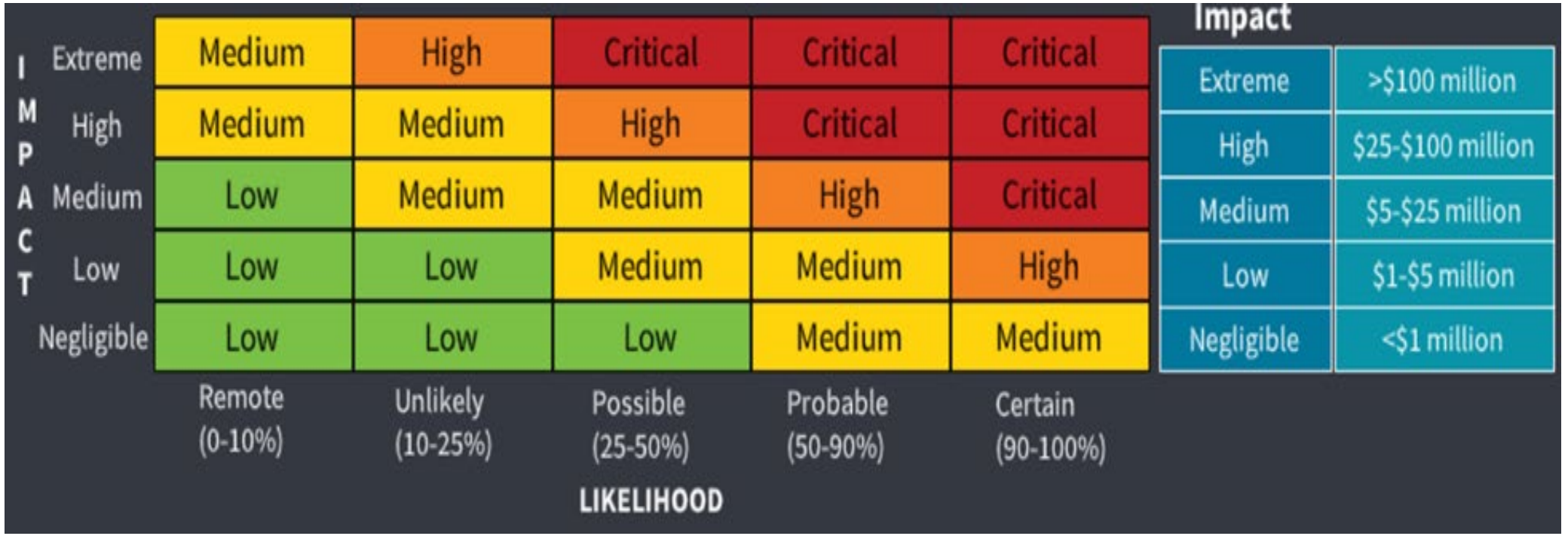



Inherent Risk
RISK
RISK
RISK
RISK
RISK
RISK
Controls
RISK
Residual Risk

Risk Prioritization



Risk Rating/Risk Matrix

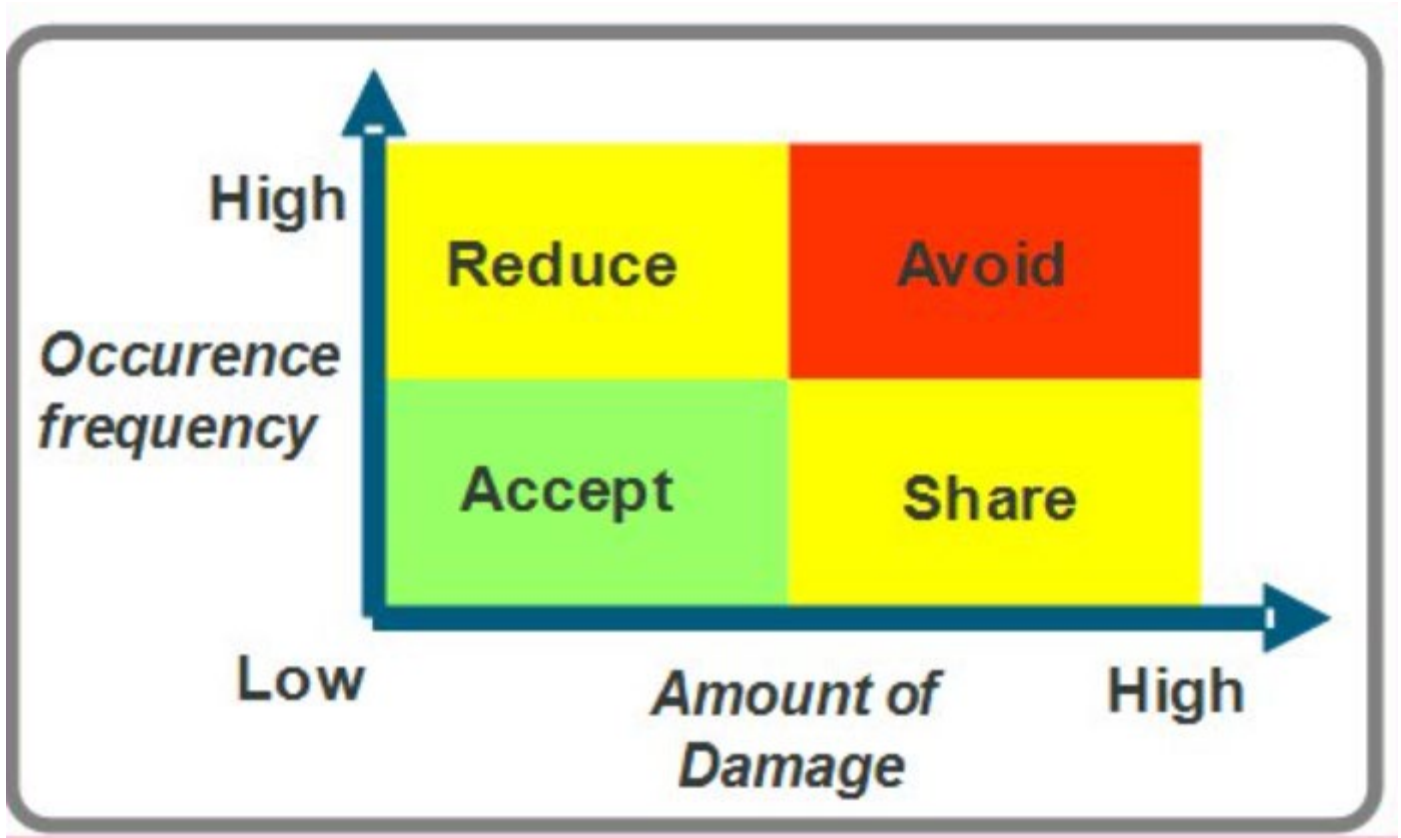


IMPACT	Remote (0-10%)	Unlikely (10-25%)	Possible (25-50%)	Probable (50-90%)	Certain (90-100%)
Extreme	Medium	High	Critical	Critical	Critical
High	Medium	Medium	High	Critical	Critical
Medium	Low	Medium	Medium	High	Critical
Low	Low	Low	Medium	Medium	High
Negligible	Low	Low	Low	Medium	Medium

LIKELIHOOD

Impact	
Extreme	>$100 million
High	$25-$100 million
Medium	$5-$25 million
Low	$1-$5 million
Negligible	<$1 million

Risk Response



IMPACT	Remote (0-10%)	Unlikely (10-25%)	Possible (25-50%)	Probable (50-90%)	Certain (90-100%)
Extreme	Medium	High	Critical	Critical	Critical
High	Medium	Medium	High	Critical	Critical
Medium	Low	Medium	Medium	High	Critical
Low	Low	Low	Medium	Medium	High
Negligible	Low	Low	Low	Medium	Medium

LIKELIHOOD

Impact	
Extreme	>$100 million
High	$25-$100 million
Medium	$5-$25 million
Low	$1-$5 million
Negligible	<$1 million

Risk Response Heat Map

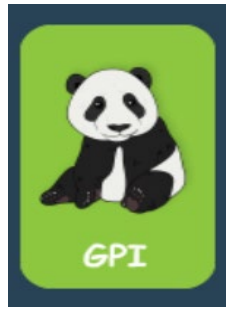
	Remote (0-10%)	Unlikely (10-25%)	Possible (25-50%)	Probable (50-90%)	Certain (90-100%)
Extreme	Reduce	Reduce Share Avoid	Reduce Share Avoid	Reduce Share Avoid	Reduce Share Avoid
High	Reduce	Reduce	Reduce Share Avoid	Reduce Share Avoid	Reduce Share Avoid
Medium	Accept Reduce	Reduce	Reduce	Reduce Share Avoid	Reduce Share Avoid
Low	Accept Reduce	Accept Reduce	Reduce	Reduce	Reduce Share Avoid
Negligible	Accept Reduce	Accept Reduce	Accept Reduce	Reduce	Reduce

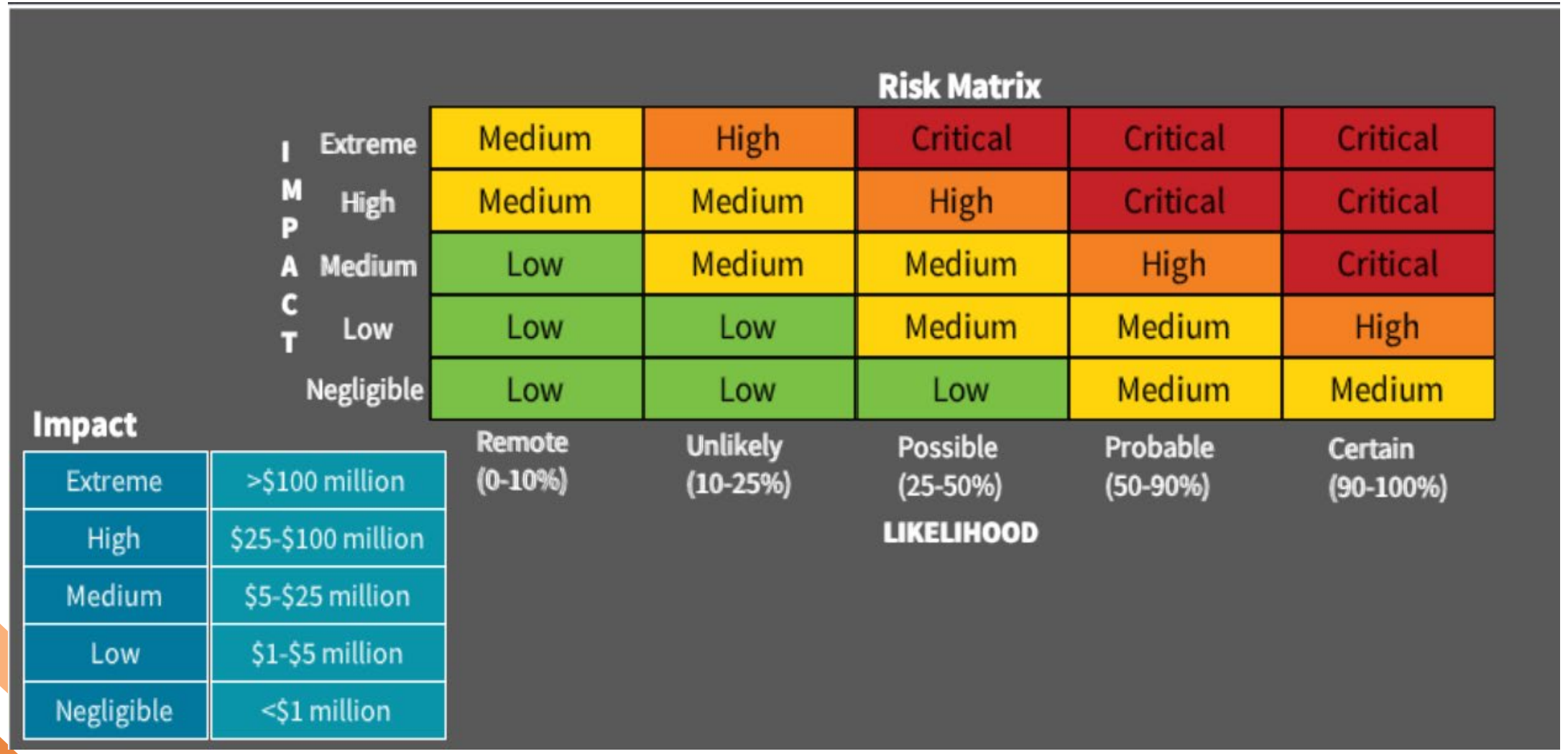
Scenario

Green Panda Insurance (GPI) has set the strategic goal of acquiring Penguin Professional Management (PPM) to achieve its mission to become a leading competitor globally.

GPI has completed the acquisition and is now setting up operations in a new international market. It is considering placing its operations center in a small region, heavily concentrated with its target customer base. This region has been recently plagued by unforeseen natural disasters. The last natural disaster occurred 3 years ago. A similar disaster occurred 3 years before that. Probability of another occurrence within the next 5 years is 70%. A natural disaster could cause an asset loss totaling $50 million

- What is the key risk? Likelihood? Impact?
- What is the risk significance? (critical, high, medium, low)
- What should be GPI's risk responses? (accept, reduce, avoid, share)




Risk Matrix
IMPACT
Extreme
High
Medium
Low
Negligible
Medium High Critical Critical Critical
Medium Medium High Critical Critical
Low Medium Medium High Critical
Low Low Medium Medium High
Low Low Low Medium Medium
Remote (0-10%)
Unlikely (10-25%)
Possible (25-50%)
Probable (50-90%)
Certain (90-100%)
LIKELIHOOD
Impact
Extreme >$100 million
High $25-$100 million
Medium $5-$25 million
Low $1-$5 million
Negligible <$1 million

Which of the following risk responses should be considered? Select all that apply.

- [ ] GPI should accept the risk rather than deploy resources that may not be needed.
- [ ] GPI should reduce the risk by implementing Disaster Recovery procedures in the region.
- [ ] GPI should continue to monitor the risk before determining if action is needed.
- [ ] GPI should avoid the risk by setting up its operations center in another region.

10 Keys to Successful Internal Audit Risk Assessments

Statement on Auditing Standards (SAS) No. 145, Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement

1. Move to a more continuous risk assessment process.
2. Address the organization's strategic risks
3. Target emerging risks
4. Consider the impact of macro-risk factors
5. Focus on cyber-risks
6. Expand input from related functions to strengthen risk assessments
7. Enhance risk assessment techniques (e.g. analytics)
8. Make your audit planning more dynamic
9. Enhance your risk reporting
10. Address management and audit committee expectations

Questions