

RISK MANAGEMENT

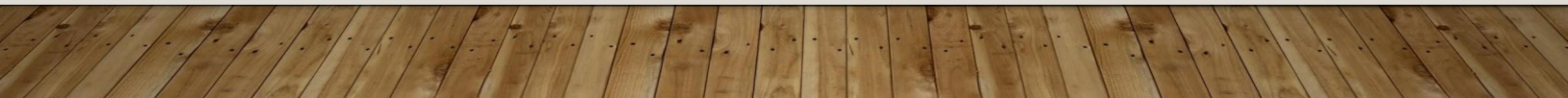
CLARE LEVISON, CPA, CGMA

LEARNING OBJECTIVES

- Understand the fundamentals of risk assessment and why it is essential
- Identify and categorize common internal and external risks
- Apply key risk management methodologies to minimize threats
- Develop and implement a risk management plan

DISCUSSION

- Describe a major business failure
- Describe the primary reasons for the failure



DEFINITIONS OF RISK

- Any event or action that adversely impacts the entity's ability to achieve its objectives
- The possibility that the occurrence of an event will adversely affect the achievement of the organization's objectives
- The effect of uncertainty on objectives
- The notion that a firm may experience events or circumstances that create a threat to its ability to continue operating

KEY TAKEAWAYS

- Risk = Uncertainty + Impact
- Can be internal or external
- Range includes negative risks (threats) & positive ones (opportunities)

ELEMENTS OF RISK



Event or hazard



Likelihood
(probability)



Consequences
(impact / severity)



Uncertainty &
assumptions



Objectives



RISK ASSESSMENT PROCESS

RISK ASSESSMENT PROCESS



INTERNAL VULNERABILITIES

- TECHNICAL

- Unpatched or outdated systems
- Default or weak passwords
- Misconfigured systems
- Access control weaknesses
- Surveillance & detection gaps

RECOMMENDED ACTIONS

- Enforce patch management & update schedules consistently
- Improve password policies, multi-factor authentication, & access reviews
- Implement security training
- Conduct periodic audits over sensitive access
- Conduct periodic audits over surveillance

INTERNAL VULNERABILITIES

– BUSINESS PROCESSES

- Segregation of duties failures
- Poor of incomplete recordkeeping & reconciliation
- Manual processes & human error
- Poor monitoring & lack of oversight
- Override or circumvention of controls

RECOMMENDED ACTIONS

- Enforce segregation of duties
- Automate where possible
- Tighten access control
- Monitor & audit regularly
- Establish clear escalation policies

INTERNAL VULNERABILITIES

– PERSONNEL

- Malicious insiders
- Negligent insiders
- Behavioral & psychological
- Financial & personal stress
- Inadequate training

RECOMMENDED ACTIONS

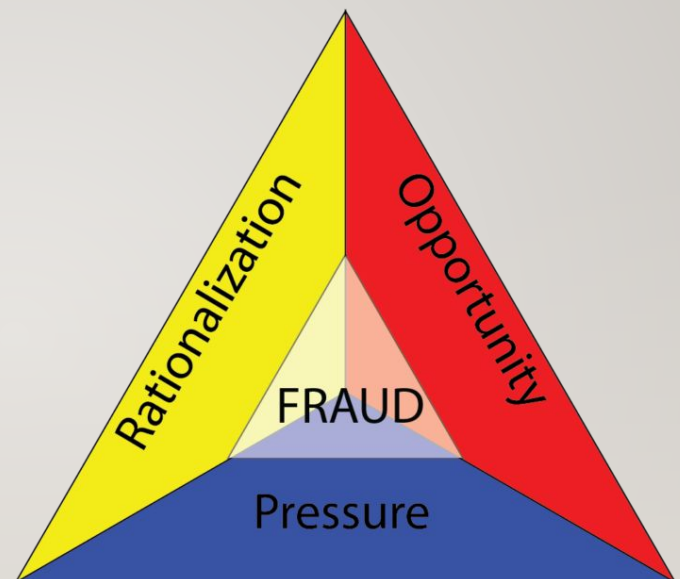
- Implement monitoring systems and role-based access controls
- Enforce policies consistently and fairly; include in performance reviews
- Improve employee engagement, compensation, and work environment
- Foster open communication, recognize performance, and support employee well-being
- Provide regular training on security, ethics, compliance, and company policies

INTERNAL VULNERABILITIES

– FRAUD

- Segregation of duties gaps
- Weak internal controls & oversight
- High-risk operational areas
- Financial pressure & rationalization
- Inadequate fraud detection & monitoring

FRAUD TRIANGLE




INTERNAL VULNERABILITIES - QUESTIONS

- Access & privilege management:
 - Who has access to critical systems? Are permissions reviewed and revoked promptly?
 - How regularly are passwords updated?
 - Do we enforce least privilege and separate duties for high-risk transactions?
- Segregation of duties:
 - Are there any roles allowing a single person to request, authorize, and reconcile transactions?
 - Do we regularly test and report on segregation of duties conflicts in key systems?

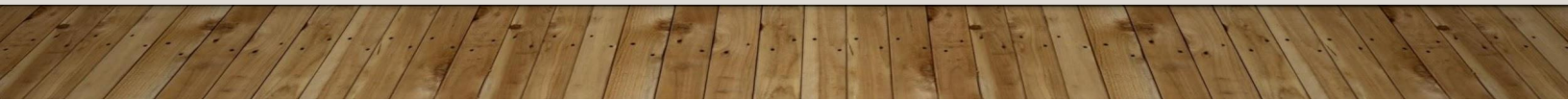


INTERNAL VULNERABILITIES - QUESTIONS

- Process & control integrity
 - Are recordkeeping and reconciliation processes complete, timely, and accurate?
 - How often are internal audits or control self-assessments done, and by whom?
 - System configuration & patch management
 - Which systems are scanned internally for vulnerabilities, and how frequently?
 - Are firmware and software patches applied promptly after release?
- 

INTERNAL VULNERABILITIES - QUESTIONS

- Employee behavior & security awareness
 - Do employees regularly receive training or phishing tests to reinforce cyber awareness?
 - Are audit logs in place, and is there monitoring for unusual behavior?
- Incident response & reporting
 - Do we have clearly documented processes to detect, report, and respond to incidents?
 - Are users encouraged and empowered to report potential security or fraud issues?



EXTERNAL VULNERABILITIES

- Economic factors
- Competitive threats
- Regulatory & legal risks
- Supply chain disruptions

EXTERNAL VULNERABILITIES

- Technological changes
- Environmental risks
- Social & political instability
- Reputation risks

DISCUSSION

- Identify the top five risk factors that could affect your organization in the next two years.

METHODS FOR IDENTIFYING RISKS



Brainstorming



Interviews



Checklists



SWOT
analysis



Root cause
analysis

METHODS FOR IDENTIFYING RISKS



Historical data
review



Expert
judgment



Scenario
analysis



Risk
workshops




Document
reviews

DEFINING RISK TOLERANCE


- The degree of variability in outcomes or level of risk that an individual or organization is willing to accept in pursuit of its objectives
- Key points:
 - Subjective
 - Context-specific
 - Influences decision-making
 - Linked to risk appetite




DEFINING RISK TOLERANCE - QUESTIONS

- What level of loss or negative impact are you willing to accept?
 - How much uncertainty or variability in outcomes is acceptable?
 - What is the maximum risk exposure you can sustain without jeopardizing core operations or goals?
 - Are there risks you absolutely cannot accept under any circumstances?
 - How do past experiences with risks influence your comfort level with current or future risks?
- 

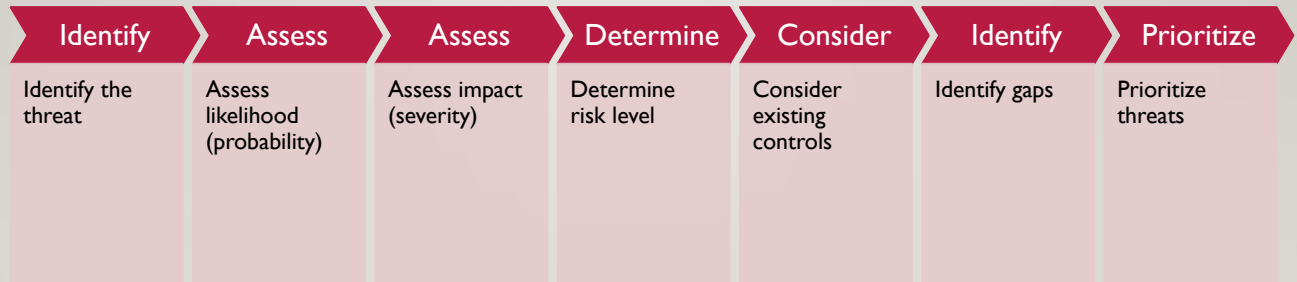
DEFINING RISK TOLERANCE - QUESTIONS

- How quickly can you recover from a potential risk event (financially, operationally, or reputationally)?
 - What is your organization's or your personal appetite for taking risks to achieve potential rewards?
 - Are there regulatory or legal boundaries that limit your risk tolerance?
 - How does your risk tolerance change under different scenarios (e.g., economic downturn, competitive pressure)?
 - How much risk are stakeholders, customers, or partners willing to tolerate?
- 

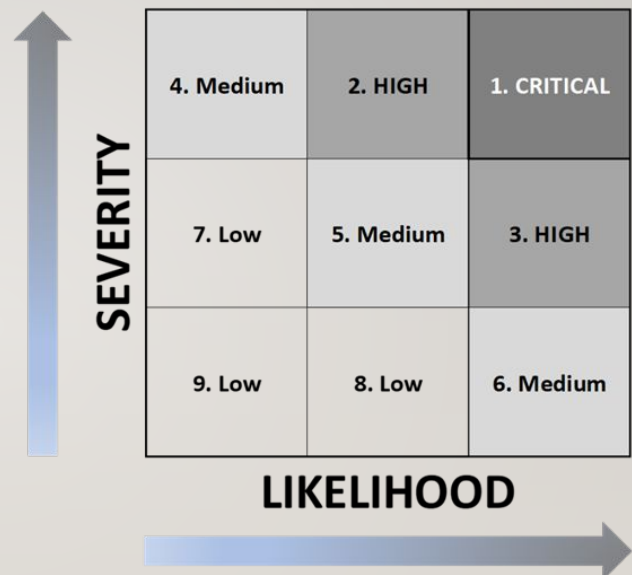
CALCULATING RISK TOLERANCE

- Identify the risk metric
 - Determine the maximum acceptable loss or impact
 - Set thresholds:
 - Risk Tolerance = Maximum Acceptable Impact / Total Exposure
 - Example: Financial Risk Tolerance
 - Company revenue: \$5 million/year
 - Maximum acceptable loss from a risk event: \$250,000
 - Risk tolerance = $\$250,000 / \$5,000,000 = 0.05$ (or 5%)
 - This means the company can tolerate financial risks up to 5% of its revenue.
- 

EVALUATING THREATS



HEAT MAP



IMPACT EVALUATION

Identify	Measure	Quantify	Consider	Evaluate	Use
Identify areas affected	Measure severity	Quantify where possible	Consider intangible effects	Evaluate time frame	Use impact ratings or scales



RISK ANALYSIS WORKSHEET

Risk ID	Risk Description	Likelihood (1–5)	Impact (1–5)	Risk Rating (L x I)	Mitigation Strategy	Owner	Status
R1	Example: Data breach due to weak passwords	4	5	20	Enforce strong password policy, implement MFA	IT Manager	Monitoring
R2	Supplier delay in delivery	3	4	12	Identify backup suppliers, improve contracts	Procurement	In Progress
R3	Key employee resignation	2	5	10	Develop succession plan, cross-train staff	HR Manager	Planned

RISK RESPONSE



Avoidance



Mitigation
(reduction)



Transfer



Acceptance

RISK RESPONSE



Exploit for
opportunities



Enhance for
opportunities



Share for
opportunities

RISK MANAGEMENT MONITORING

- The ongoing process of tracking identified risks, detecting new risks, and evaluating the effectiveness of risk responses over time
- Key objectives:
 - Track changes in risk likelihood or impact
 - Assess the effectiveness of mitigation or response plans
 - Identify new or emerging risks
 - Ensure accountability by confirming that owners are addressing assigned risks
 - Support decision-making with up-to-date risk information

QUESTIONS

