Practical Enterprise Risk Management

September 25, 2023 ACUA Presentation

By Alex Tzoumas, CRMA, CIA, CFE, CISA, CDPSE

Who Developed the COSO Framework

The Committee of Sponsoring Organizations (COSO)

- Established in 1985 to sponsor the National Commission on Fraudulent Financial Reporting
- Committee is comprised of:
  - The Institute of Internal Auditors (IIA)
  - American Institute of Certified Public Accountants (AICPA)
  - American Accounting Association (AAA)
  - Institute of Management Accountants (IMA)
  - Financial Executives Institute (FEI)

Source: COSO.Org

COSO ERM Program Fundamentals

To ensure the achievement of the university's primary **long term strategic objectives**, management would adopt an Enterprise Risk Management (ERM) program that:

1. Systematically identifies inherent risks to strategic institution objectives and management processes to mitigate risks in line with the Board of Trustee's risk appetite.

2. Strengthens the relationship between the management of risk and the rewards of its leadership team. **(Must be part of performance evaluation)**

3. Promotes a control environment made up of an integrated system of institution governance, ethical tone-from-the-top, continuous risk assessment, employee awareness, and sound internal controls. **(Program needs a champion!)**

ERM Program Responsibilities

- **Everyone** is responsible for identifying potential risks. Management is responsible for developing risk management plans and implementing risk reduction strategies. (It's their plan) The risk management process is integrated with other planning processes and management activities. (Examples: Maintenance, Faculty Evaluations, Training, etc.)

- **President** is responsible on behalf of the Board of Trustees for establishing, implementing and maintaining a risk management system in accordance with the established ERM program and the Board of Trustee's directives. Assignment of responsibilities in relation to ERM is the prerogative of the President.

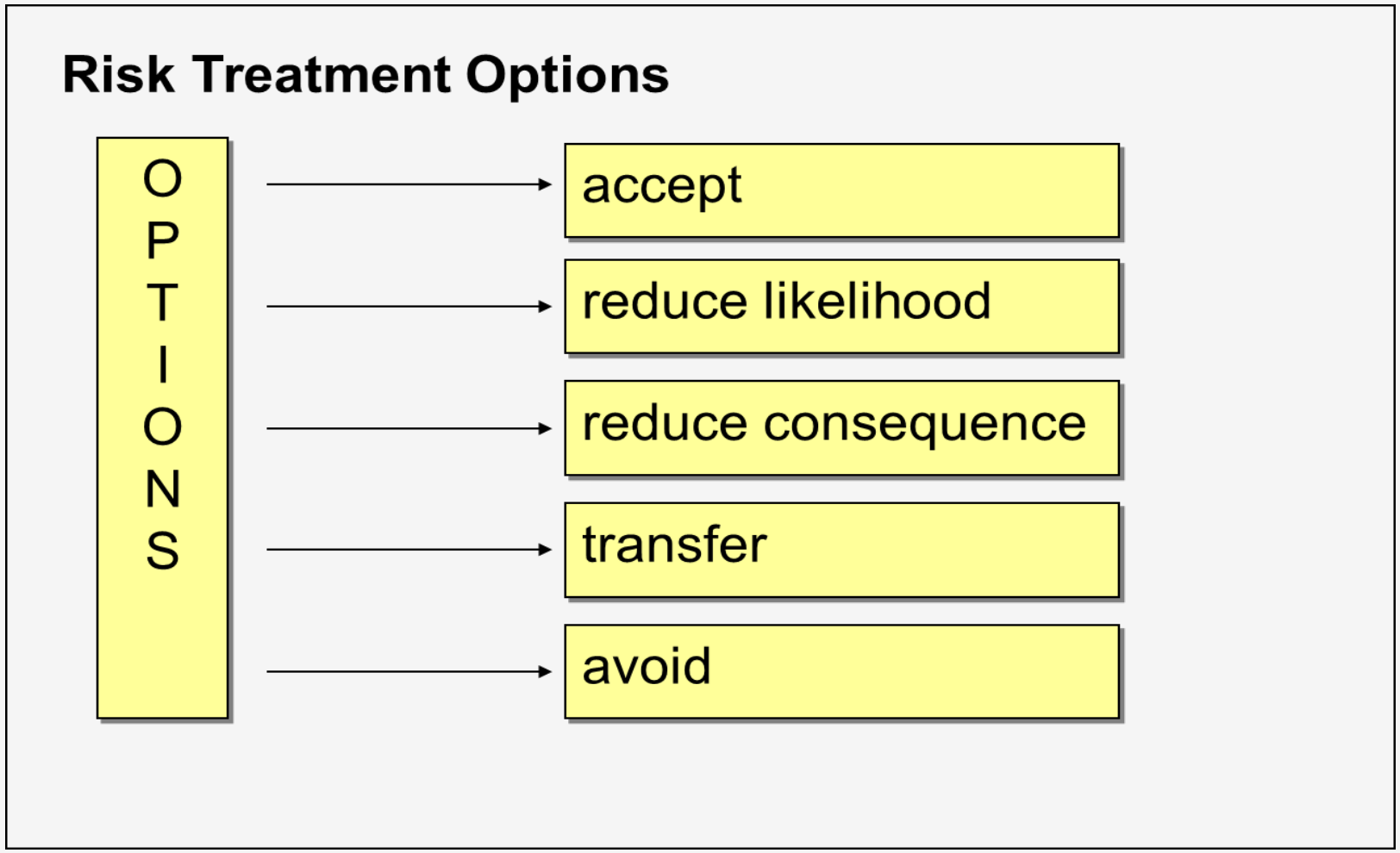
- **Board of Trustees** are responsible for oversight of the processes for the identification and assessment of the general risk spectrum and reviewing the outcomes of changes in residual risk.

- **Audit Executive** is responsible for ongoing reassessment, reporting of residual risk changes and evaluating the ERM program. **(Semi-annual presentations to Board)**

The Risk Management Process

- **Establish Context –** Method to determine acceptable level of risk (i.e. understand loss potential and adverse consequence potential) and what is that level. (Exposure x probability = loss potential)
- **Identify Vision Critical Risks –** What are the potential hazards and opportunities at risk (i.e. lower retention, lower grad rate, student harm, staff retention, loss of facility, all affect brand)
- **Analyse Risks –** Likelihood/probability and magnitude/exposure of effect on strategic objectives
- **Define Population to Continuously Monitor –** Rank and prioritize based on rating method
- **Treat Risks –** Identify and monitor management's risk mitigation action plans **(semi-annual updated)**

The Risk Evaluation Process



The Risk Identification Process

New College of Florida Risk Evaluation Form	Division / Operation / Group / etc.: Date:
Business Objective:	
Risk Category:	
Risk Description/Contributing Factors:	

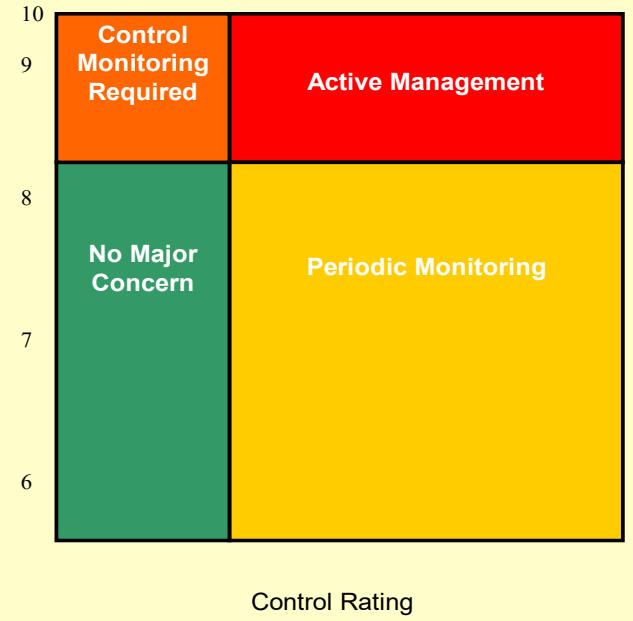
The Risk Rating Process

Inherent Risk Rating Table

Likelihood Rating -		Consequence Rating –		Inherent Risk Rating –	

If the combined rating is 7 or greater continue on to the control evaluation section.

Existing Controls



Control Rating Table

Effectiveness Rating		Application Rating		Control Rating -	

The Risk Management Process

Summary of Risk Management Plan		
Employee Responsible:	**Reviewed by:**	**Completion Timetable:**
Signature:	**Signature:**	**Next Review Required:**

ERM Program Implementation

- Obtain Audit and Compliance Committee & Executive Management Support
- Identify top 10 to 15 major strategic objectives to evaluate
- Present ERM program Risk Evaluation Forms to management for completion (most often a review and augmentation of your draft) – Include the President!
- Present Risk Evaluation Summary to Audit and Compliance Committee
- Develop and implement periodic risk status reports for Board of Trustees (see next slide)

Board Reporting

Enterprise Risk Management Analysis									
Risk Evaluation Form Title	**Business Objective**	**Inherent Risk Description**	**Inherent Risk Rating**	**Control Rating**	**Risk Ranking June 2022**	**Risk Ranking Jan 2023**	**Management's Plan to Further Mitigate Risk**	**Risk Category**	**Responsible Manager(s)**
Facilities	Provide and maintain facilities in accordance with university needs, to quality specifications, in a cost effective/competitive and regulatory compliant manner.	Significant age of buildings and budget limitations may result in facilities being disrupted or unable to fulfil university housing and administrative building needs in a timely and quality manner. Delays could cause inability to meet student body and administration demand causing a substantial loss of potential revenue, reputation and personnel dissatisfaction.	9	7	16	16	1. New College strategic plan calls for an increase in student housing fees to help address deferred student dormitory maintenance over the next 12 months. 2. Employee and student relations are being addressed by management. 3. Facility improvements and housing will remain at issue until the 70 Pei beds can be restored.	Customer Relations & Brand Recognition	AVP Facilities, CFO
Human Resources	To design and manage compensation/benefit plans and employee satisfaction strategies that cost effectively attract, retain, and heighten the abilities of highly proficient employees who consistently achieve New College's strategic goals and objectives.	Personnel leave, are ineffective, or untrustworthy exposing New College to under performance, business process interruptions, loss of institutional knowledge, misconduct and increased recruitment and training costs thus hindering the achievement of key university's objectives.	8	7	15	15	1. Implement company-wide base pay review. (Initially planned for calendar year 2021.) 2. Communication plan with all supervisors regarding expectation of open communication in each department and completion of annual performance evaluations in a timely manner. 3. Implement anonymous supervisor feedback process. Summer 2022 4. Develop an antibullying regulation. Summer 2022 5. Provide the Board with an annual Staff Views Report. Summer 2022 6. Conduct 2023 Employee Satisfaction Survey.	Business Continuity	Chief Human Officers & all Executives
Strategic Growth Initiatives	Demonstrate management's ability to achieve the university's goals of 1,200 students by 2024-25, 80% four-year graduation rate, and be recognized among the best twenty liberal arts universities in the nation.	Growth initiatives for existing or future enrolment fail to achieve projected results and support university graduation and achievement targets.	8	5	13	13	1. Market in international markets including Asia and South America to attract foreign students. 2. Improved applicant communication to facilitate higher conversion rates. 3. Add recruiter to manage student interest programs. 4. Continuously evolve curriculum to higher demand fields. 5. Manage social media posts to improve university's image. 6. Publicize research and other faculty successes.	Asset Productivity and Brand Reputation	President, Provost, VP of Enrolment Management, and Board of Trustees
Cyber Security & Reliability	Demonstrate management's ability to secure protected data, respond to all cyber security breach threats/incidents, and assure reliability and accessibility of all data processing systems and repositories.	Non-public College, personal student and/or employee information is obtained and misused by unauthorized persons resulting in remediation costs, legal expense, regulatory agency sanctions and/or brand reputation damage. Data processing systems cannot be accessed or data lacks integrity.	8	5	13	13	1. Breach response team, which includes the CFO, Chief Audit Executive, Director of Application Support & Development, Director of Information Technology, and Director of Technology Support will evaluate known causes for cyber related losses and enhance policies and process controls to further reduce exposures. 2. Penetration test will be performed during the 21/22 fiscal year. 3. External mail may be flagged to help College personnel recognize phishing attacks. 4. IT is in the process of implementing ISO 27001 Information Security Management to lessen cyber exposures.	Asset Security, Regulatory Compliance and Brand Reputation	Director of Application Support and Development, CFO, Director of Technology Support
Business Contunity	In the event of an emergency, imminent threat, or disaster, be prepared to identify the risk, quickly respond to minimize harm, and expeditiously restore normal university operations. Develop and Maintain an Emergency Operations Plan that assures the university is continuously able to safely and efficiently educate, conduct research, operate campus services, house students, communicate, and recruit.	Campus community is harmed and/or university operations are disrupted in a manner which adversely impacts the university's ability to maintain a safe environment, delivery its services, preserve public trust, and/or achieve its strategic objectives. 1. Critical business systems become inoperable (i.e. communications, payment processing, financial reporting, information or internet access). 2. Facilities become uninhabitable, unavailable, or destroyed. 3. Students cannot safely attend classes or reside in dorms. 4. Faculty or staff cannot perform essential job functions. 5. Campus support services such as the cafeteria or maintenance cannot provide services. 6. The campus cannot be accessed.	6	7	13	13	Risk Management Plan - Campus will evaluate and improve continuity preparations as follows: 1. Develop Executive Security Program, 2. Assemble disaster recovery teams and emergency response wardens for all buildings/locations, 3. Conduct severe incident response drills and table top exercise with all campus personnel and a tiered involvement with students to improve awareness and response, 4. Update/renew POs with critical disaster response supply vendors, 5. Develop standing communiques to inform public of emergency status.	Business Continuity (also see Cyber Security, Facilities, & Environmental Safety)	CFO

2013 COSO Framework - Principle Coverage Analysis

Framework Principles:

- Control Environment:
  1. The organization demonstrates a commitment to integrity and ethical values (Code).
  2. The Board of trustees demonstrates independence from management and exercises oversight of the development and performance of internal control (Audit Dept Reporting).
  3. Management establishes, with board oversight, organizational structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
  4. The organization demonstrates a commitment to attract, develop, and retain competent individuals.
  5. The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.
- Risk Assessment:
  6. The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
  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 (Risk Evaluation Forms).
  8. The organization considers the potential for fraud in assessing risks to the achievement of objectives (ACFE).
  9. The organization identifies and assesses changes that could significantly impact the system of internal control.

2013 COSO Framework - Principle Coverage Analysis

- Control Activities:
  10. The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels. (Risk Evaluation Forms)
  11. The organization selects and develops general control activities over technology to support the achievement of objectives. (ITGCs)
  12. The organization deploys control activities through policies that establish what is expected and procedures that put policies into action. (Updates & Training)
- Information and Communication:
  13. The organization obtains or generates and uses relevant, quality information to support the functioning of internal control. (Standard vs. custom reports)
  14. The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control. (Audit & Compliance Partners – who owns what)
  15. The organization communicates with external parties regarding matters affecting the functioning of internal control. (Audit reports to Inspector General & External Auditors)
- Monitoring Activities:
  16. The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning. (Process narratives with integrated controls)
  17. The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the Board of Trustees, as appropriate.

Shape Risk Management Control Environment

- **Everyone** demonstrates an acceptance of risk mitigation, control, and compliance responsibilities.
- **Management** maintains an ethical tone-from-the-top. Routinely monitors controls/ mitigation strategies and accordingly integrates controls to mitigate inherent process and system risks. **Assigns control responsibilities to qualified personnel.**
- **Chief Audit Executive** reliably and systematically evaluates controls and progress in accordance with professional standards. Adjusts Risk Evaluation Forms for **deficiencies** and reports to management and the Audit and Compliance Committee.
- **Audit and Compliance Committee** evaluates authenticity of efforts and adequacy of resources dedicated to risk management, ethical standards, and achieving sound institution governance.

Presentation Summary

- ERM program needs a champion and everyone's attention
- Need an efficient method to identify and monitor potential impairments to achieving strategic objectives
- Put the issue in-front of the decision makers and influencers
- Follow the framework to avoid oversights
- Continuously update the Risk Evaluation Forms
- Take the decision makers out to lunch and build a relationship

Population of Strategic Objectives

Strategic Objectives and Emphasis vary for every institution!

- **To operate in a legal and ethical manner, build the university's reputation, and minimize the cost of, or loss from, litigation.**
- **To design and manage compensation/benefit plans and employee satisfaction strategies that cost effectively attract, retain, and heighten the abilities of highly proficient employees who consistently achieve the university's strategic goals and objectives.**
- **Provide and maintain facilities in accordance with university needs, to quality specifications, in a cost effective/competitive and regulatory compliant manner.**
- **Create and communicate a tone of ethics, integrity, and awareness from the top of the organization that sponsors a high level of ethical conduct and regulatory compliance.**

Preliminary Population of Objectives

- **Ensure financial results, required footnotes and other disclosure information are reported and presented in a complete, accurate, timely, consistent, fair manner as required by the Government Accounting Standards Board and applicable regulatory guidelines.**
- **Demonstrate management's ability to achieve the university's goals of ____ students by 2024-25, ___% four-year graduation rate, and be recognized among the best ____ liberal arts universities in the nation.**
- **Demonstrate management's ability to secure protected data, respond to all cyber security breach threats/incidents, and assure reliability and accessibility of all data processing systems and repositories.**

Preliminary Population of Objectives

- **To operate the university campus in a safe and secure manner such that personnel, students and visitors feel safe, the university's reputation is supported, costs related to bodily and property harm are minimized, liability insurance rates are the lowest possible, and litigation is minimized.**
- **Accurately adjust strategic plans, forecasts, and budgets for economic and/or political events in order to minimize the impact of uncontrollable shifts in State funding, enrolment, operational costs, and other economic dependent variables.**
- **Build and maintain a competitive and compliant business model to increase revenues from a variety of sources, achieve the university mission, expand university recognition in support of opportunities for continuous growth.**