Enterprise Risk Management at the State University of New York: A Benchmark for Saudi Universities

Said Malki
State University of New York

Naif Khalid Aldwais
Prince Sattam Bin Abdulaziz University

Universities face constantly a variety of risks, including strategic, financial, operational, compliance, and reputational risks. To help ensure goals and objectives are met, universities must manage these risks. While some organizations manage risk using an informal process, others have a formalized structured approach. Enterprise Risk Management, ERM, is a formal and continuous process that is designed to identify, assess, prioritize, and manage all risks and opportunities for an institution. The study proposes the use of ERM processes as used in the State University of New York as a benchmark or a reference for Saudi Universities.

Keywords: Traditional Risk Management, Enterprise Risk Management, Risk Exposure, Internal Control

INTRODUCTION

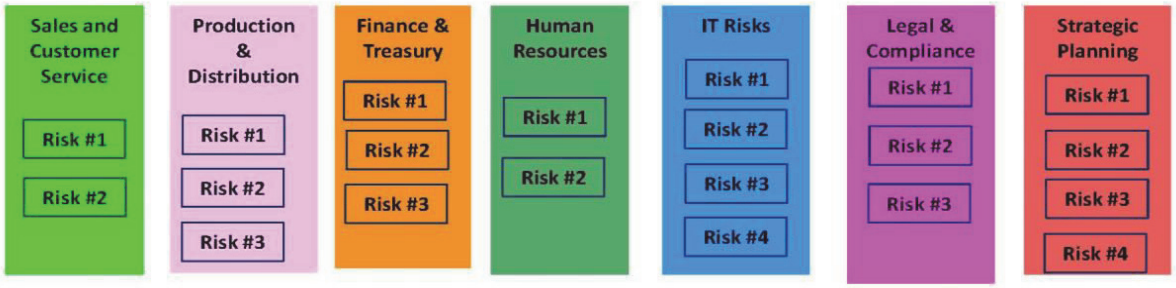
Traditionally, organizations manage risks by placing responsibilities on business unit leaders to manage risks within their areas of responsibility. For instance , the Chief Technology Officer (CTO) is responsible for managing risks related to the organization's information technology (IT) operations, the Treasurer is responsible for managing risks related to financing and cash flow, the Chief Operating Officer is responsible for managing production and distribution, and the Chief Marketing Officer is responsible for sales and customer relationships, and so on (Beasley, 2012). The first portion of this paper focuses on the description of ERM framework and its suitability for Saudi universities. The second portion of the paper proposes ERM as implemented by the State University of New York as a benchmark, a field of exploration or, a reference for Saudi universities.

DESCRIPTION OF ENTERPRISE RISK MANAGEMENT AND ITS SUITABILITY FOR SAUDI UNIVERSITIES

While assigning functional experts' responsibility for managing risks related to their business unit is useful, the traditional approach to risk management has drawbacks. Indeed, the are consistent risks on the horizon that may go undetected by management and that might affect the organization. Let's summarize these limitations (Beasley, 2016):

- There may be risks that "fall between the siloes" that none of the silo leaders can see. Risks don't follow management's organizational chart and, as a result, they can emerge anywhere in the business. As a result, a risk may be on the horizon that does not capture the attention of any of the silo leaders causing that risk to go unnoticed until it triggers a catastrophic risk event.
- Some risks affect multiple siloes in different ways. So, while a silo leader might recognize a potential risk, he or she might not realize the significance of that risk to other aspects of the business. A risk that seems relatively harmless for one business unit, might actually have a significant cumulative effect on the organization if it were to occur and impact several business functions simultaneously.
- An individual silo owner may not understand how an individual response to a particular risk might impact other aspects of a business. For example, in reaction to growing concerns about cyber risks, the IT function may tighten IT security protocols but in doing so, employees and customers find the new protocols confusing and frustrating, which may lead to costly work-arounds or even the loss of business.
- Management may focus more on risks related to internal operations inside the walls of the organization with a limited attention on risks that might emerge externally from outside the business. An organization may not be monitoring a competitor's move to develop a new technology that has the potential to significantly disrupt how products are used by consumers.
- The development and execution of the organization's strategic plan may not give enough consideration to risks especially when leaders of traditional risk management functions have not been involved in the process.

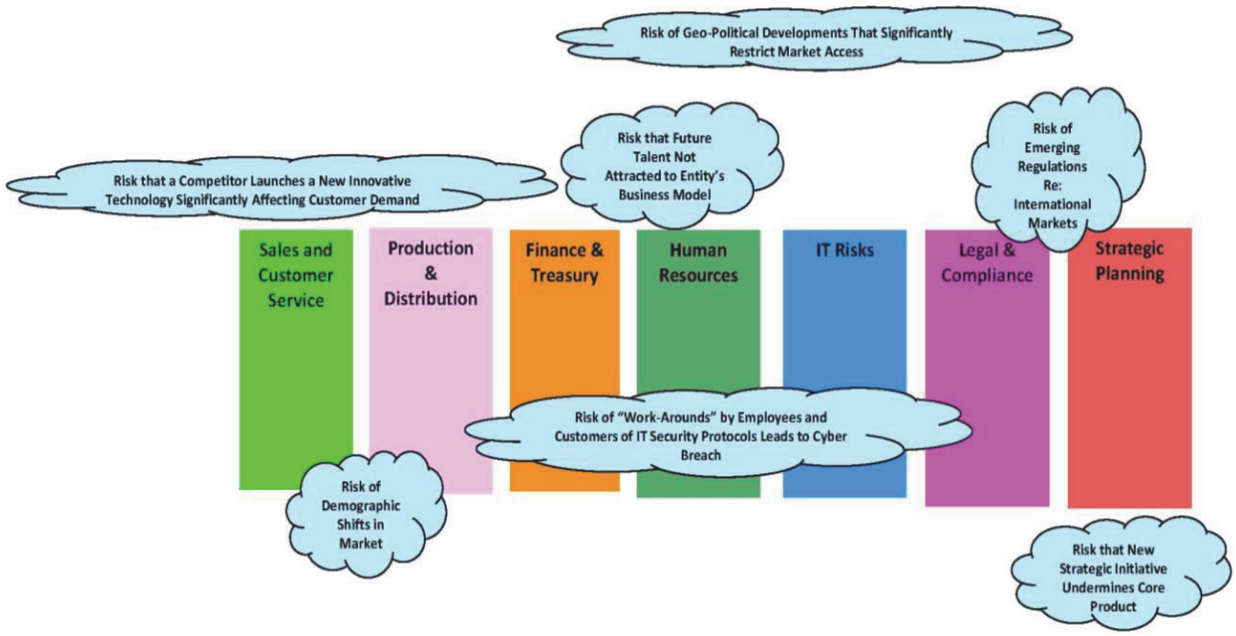
FIGURE 1
TRADITIONAL RISK MANAGEMENT APPROACH



"Silo" or "Stove-Pipe" Risk Management

Source: Beasley (2016)

FIGURE 2
LIMITATIONS OF TRADITIONAL RISK MANAGEMENT



Source: Beasley (2016)

While assigning functional experts' responsibility for managing risks related to their business unit is useful, the traditional approach to risk management has drawbacks. Indeed, the are consistent risks on the horizon that may go undetected by management and that might affect the organization. Let's summarize these limitations (Beasley, 2016):

- There may be risks that "fall between the siloes" that none of the silo leaders can see. Risks don't follow management's organizational chart and, as a result, they can emerge anywhere in the business. As a result, a risk may be on the horizon that does not capture the attention of any of the silo leaders causing that risk to go unnoticed until it triggers a catastrophic risk event.
- Some risks affect multiple siloes in different ways. So, while a silo leader might recognize a potential risk, he or she might not realize the significance of that risk to other aspects of the business. A risk that seems relatively harmless for one business unit, might actually have a significant cumulative effect on the organization if it were to occur and impact several business functions simultaneously.
- An individual silo owner may not understand how an individual response to a particular risk might impact other aspects of a business. For example, in reaction to growing concerns about cyber risks, the IT function may tighten IT security protocols but in doing so, employees and customers find the new protocols confusing and frustrating, which may lead to costly work-arounds or even the loss of business.
- Management may focus more on risks related to internal operations inside the walls of the organization with a limited attention on risks that might emerge externally from outside the business. An organization may not be monitoring a competitor's move to develop a new technology that has the potential to significantly disrupt how products are used by consumers.
- The development and execution of the organization's strategic plan may not give enough consideration to risks especially when leaders of traditional risk management functions have not been involved in the process.

The objective of enterprise risk management is to develop a holistic, portfolio view of the most significant risks to the achievement of the entity's most essential objectives. The "e" in ERM signals that ERM seeks to create a top-down, enterprise view of all the significant risks that might impact the business. In other words, ERM attempts to create a basket of all types of risks that might have an impact – both positively and negatively – on the viability of the business.

Because risks constantly emerge and evolve, it is important to understand that ERM is an ongoing process. It is not about a mere project that has a beginning and an end. While the initial launch of an ERM process might require aspects of project management, the benefits of ERM are only realized when management thinks of ERM as a process that must be active and alive, with ongoing updates and improvements. The diagram below shows the core elements of an ERM process.

FIGURE 3
ERM FRAMEWORK

Source: Beasley (2016)

According to this framework, the organization has an annual ERM cycle which is facilitated by the ERM team. The ERM team may consist for instance of three members, the Director and two analysts. They are the link between the members of the organization responsible for risk management and the enterprise risk management process. The annual process begins with the identification and assessment of risks in the January / February time frame. The ERM team administers a survey to Vice Presidents (VPs) and selected Directors. In the meantime, interviews are conducted with the CEO and the CEO's direct reports (Do, & others, 2016).

The ERM team analyzes the information gathered in the surveys and interviews to prioritize the risks. The prioritized risks are typically presented using a heat map. For each of the organization's top risks (typically 8-10 risks), an owner is identified. The risk owners, also referred to as risk champions, are responsible for assigning a risk manager, approving mitigation (action) plans, resourcing the plan, and briefing the plan to the Board. The risk owners are assisted by risk managers who are responsible for the risk action plan. The ERM team works with the risk managers to understand survey findings and develop mitigation plans. The risk managers are responsible for managing the risk and tracking the progress of the mitigation plan. They own the risk and report progress of the mitigation plans to the ERM team on a quarterly basis. The ERM team summarizes the risks, the risk mitigation plan and the progress in implementing the plans on a dashboard that is reported to executive leadership and the Board (Do & others, 2016).

FIGURE 4
EXAMPLE OF ERM & STRATEGY IMPLEMENTATION TIMELINE

Source: NCSU.edu

The strategic planning process and ERM process are initiated in two different organizations and start at slightly different times. Strategic planning starts with the CEO and strategy leads. ERM starts with surveying the VPs and their direct reports. The two processes operate in parallel, with both following an annual cycle and combined top-down / bottoms-up approach. There are several points where information is shared between the two. This is how the company integrates the two processes to ensure ERM and strategy are in sync and have an enterprise wide impact. The following are the specific points of integration:

- Macro Level – The first point of integration is the third quarter risk update. This updated information, which includes external risk developments that may impact the organization, is communicated to the corporate strategy team who then factors the information into the corporate-level strategy.
- Micro Level – The second stage of integration is at the business unit level. Each business unit receives the broad strategic objectives post the CEO and VPs meeting (January/ February time frame). The business units also receive specific information about their top risks from the ERM team (March time frame). The business units factor this information into the formulation of their strategic plans.
- Third Level – The final stage of integration occurs when Functions develop strategies/ action plans to support Business Unit plans and address specific risks.

With respect to ERM components and related survey measures, they are outlined in the table below:

TABLE 1
ERM COMPONENTS AND RELATED SURVEY MEASURES

Component	Survey Item
Objective Setting	1. Has aligned its business risks with its corporate-level and business-unit-level goals and objectives 2. Has established explicit, corporate-wide risk tolerance levels or limits for all major risk categories 3. Has clearly communicated its expectations for risk-taking to senior managers
Identification	1. Has established a comprehensive business risk inventory of the risks you expect your managers to manage 2. Its business units utilize facilitated self-assessment and/or survey techniques to map risks
Risk Reaction	1. Conducts formal risk assessment across the company on a regular basis 2. Its business units analyze the root cause, impact, and interrelationships of its risks 3. Has quantified its key risk to the best extent possible 4. Has a process to integrate the effects of the major risk types (strategic, operational, financial, hazard, and legal) 5. Its business units develop and determine risk mitigation strategies
Oversight	1. Has established written risk policy and procedure manuals that are consistent across major risks 2. Its business units monitor and report on current status of managing key risks 3. Has identified the key metrics required for reporting on risk management performance
Information and Communication	1. Has a corporate-wide common language for communicating risk-type exposures, control activities, and monitoring efforts 2. Has regular briefs to the board and executive committee on risk management issues
Internal environment	1. Has communicated a risk management mission statement, value proposition, and benefits statement to senior managers 2. Has incorporated responsibility for risk management into the position description of all managers 3. Board of directors or committee of the board is actively involved in the risk management process
Management	1. Perceived benefit of ERM on company's general management consensus 2. Perceived benefit of ERM on company's ability to make better-informed decisions 3. Perceived benefit of ERM on company's ability to articulate and communicate risk taking to the management board and outside stakeholders 4. Perceived benefit of ERM on increased company management accountability

Component	Survey Item
Performance	1. Perceived benefit of ERM to measure risk-adjusted performance among business units 2. Perceived benefit of ERM to increase ability to meet strategic goals 3. Perceived benefit of ERM to reduce earnings volatility 4. Perceived benefit of ERM to increase profitability

Source: Gates. S & others (2012)

In total, ERM programs differ from previous approaches to risk management in several ways. Specifically, ERM programs (Rejda & others, 2020):

- Encompass all areas of an organization's exposure to risk, including financial risk, operational risk, strategic risk, hazard risk, and additional risks, as well.
- Prioritize and manage the risks an organization faces considering a portfolio approach rather than viewing the risks in isolation.
- Evaluate the risk portfolio relative to internal and external environments, stakeholders, systems, and circumstances.
- Recognize that risks across an organization are inter-related, and that the combined exposures differ from the sum of the individual exposures.
- Provide a structured process for managing all risks, whether the risks are qualitative or quantitative in nature.
- View the effective management of risks as a competitive advantage.
- Embed risk management throughout the organization so that it becomes a component in all major decisions made by the organization.

Once the ERM plan is implemented, the process is sensitive to the internal and external environment. A two-way flow of information occurs from the process to internal parties who are responsible for (or "own") various risks. They inform the enterprise risk management process, and in turn are informed by the process. As the diagram below indicates, the process is continuous. The output from the process is fostered strategic decision making and to get started, the ERM plan must be implemented (Rejda & others, 2020).

Evidence on successful ERM implementation reveals several central factors. First, for the program to be successfully implemented, there must be commitment from the management team. Although a board of directors may approve or mandate implementation of an ERM program, the corporate officers are responsible for seeing that the program is implemented. Commitment of the management team and other key organizational leaders is essential for acceptance of the program. As a reflection of the importance of the risk management function, some organizations have created a "C-suite" level position, Chief Risk Office (CRO). The Chief Risk Officer (CRO) is responsible for the treatment of all the risks facing the organization, and for creating a program to successfully manage these risks. A second crucial factor in ERM implementation is communication. The benefits of ERM and the ERM framework must be communicated to lower-level managers and employees of the organization. Risk ownership—who is responsible for various aspects of the ERM plan—must also be communicated. Keeping the plan simple and starting small are important during the implementation stage, and frequent updates on the status of implementation are vital during the adoption stage (Goni, 2018).

After this concise presentation of the definition and components of ERM, it is essential to note that there are limited research studies on the determinants of this process adoption and its ability to create value for organizations headquartered in Middle Eastern countries. Specifically, few ERM studies have been conducted for organizations in Saudi Arabia. In this regard, one can refer though to the empirical study by Alzharani and Aljaaidi (2015) that investigates the effectiveness of audit and risk management committees in Saudi Arabia and the exploratory study by Hain (2011) that investigates risk perception and risk management strategies of Western multinational enterprises in the Middle East. Particularly, Alzharani and Aljaaidi's study covers one hundred and two publicly listed Saudi organizations, in which the researchers

assert that individuals with an internal audit background would have the relevant knowledge about risk management practices in Saudi organizations. The main reason for this conclusion is that the responsibilities of monitoring and controlling risk management activities are closer to the audit committee than to the board of directors or other committees in Saudi organizations.

In this regard, Davenport and Bradley (2001) indicate that the leaders who are critical for an ERM initiative to succeed are often CFOs, risk managers or leaders from the internal audit. It is evident that some organizations might not appoint a CRO to lead ERM activities; instead leaders from other functions such as internal audit or finance, might take the initiative to lead ERM activities. Therefore, including participants with a leadership role in internal audit and finance helps to provide some level of objectivity in the responses given since these participants usually have a better understanding of ERM implementation in their organizations. In sum, the literature review reveals a limited amount of research studies exploring ERM implementation in organizations headquartered in Middle Eastern countries (Aliesa, 2017).

In this regard, a study by Rao and Marie (2007) uses a survey questionnaire to explore ERM implementation in hundred business organizations in Dubai. The survey questionnaire covers five components of the Committee of Sponsoring Organizations COSO framework, namely, control environment, risk assessment, control activities, information and communication, and monitoring. The researchers explore the status of ERM implementation in terms of the tools and processes used by companies in Dubai to identify and measure risks. The research results reveal that respondents are generally satisfied with the existing tools for assessing, measuring and mitigating financial risks, such as credit risks, interest rate risks and reinvestment risks. Nevertheless, the level of satisfaction in terms of managing operational risks (e.g., reputation, technology, intellectual capital, political and regulatory and catastrophe) is mixed. Moreover, culture, time availability and cost are classified as key barriers to ERM implementation. Although the research results reveal that key aspects of risk management are adequately implemented, the researchers highlight the need for organizations in Dubai to implement integrated strategic ERM processes and to increase awareness about ERM. They also suggest five strategic steps to improve ERM implementation. However, the researchers indicate that these findings are limited to businesses in Dubai due to the small size of the study's sample.

Another study by Muralidhar (2010), using six case studies, explores the status of ERM implementation for selected entities in the oil and gas industry in six countries. The researcher identifies key determinants of ERM adoption, explores challenges to ERM implementation and recommends an implementation plan to establish a robust ERM framework specific to entities in the Gulf region. He uses an inductive research approach based on semi-structured interviews by asking open-ended questions (who, why, what and how) to explore participants' answers to research objectives. The researcher uses the data collected to position organizations in the ERM maturity model according to their ERM implementation progress as under construction, partial or a complete ERM framework in place. The research findings reveal that ERM means different things to oil and gas companies in the Middle East, and the key emerging themes in ERM implementation are standardization, integration and centralization. In addition, the key determinants of ERM adoption are corporate governance, leadership of the chief executive, good business practice, initiative of the board of directors and internal audit recommendation (Muralidhar, 2010).

It is evident that the empirical evidence on ERM implementation for organizations that operate in Middle Eastern countries provides insights into the key determinants of ERM adoption and the challenges to implementing ERM (Muralidhar, 2010). This evidence also sheds light on the importance of ERM for Dubai businesses, the types of risks critical for these businesses and the adequacy of tools and processes to manage business risks (Rao and Marie, 2007). However, researchers neither apply a structured approach to identify organizations embracing ERM nor use specific measures to explore the degree of ERM implementation, similar to empirical studies conducted for Western organizations.

There are several visionary Saudi universities that are emerging internationally in the areas of research, teaching excellence, and continuous improvement. Nevertheless, more focus should be given to ERM by Saudi universities top managers and leaders. For instance. an overview of the strategic plan of leading Saudi universities such as King Fahd University of Petroleum & Minerals and King Saud University reveals the absence of ERM analysis despite its importance.

Saudi Arabia is a member of the G20 and its economic role is crucial at the international level. Furthermore, Saudi universities and colleges reflect a clear awareness in regards to continuous improvement and international accreditation standards. In this context, the adoption of ERM appears to be a necessity for Saudi educational organizations. The second portion of the paper proposes the State University of New York ERM as a reference, a benchmark, or an area of exploration by Saudi universities.

The State University of New York (University) recognizes a variety of risks including strategic, financial, operational, compliance, and reputational risks, and is committed to implementing and utilizing an Enterprise Risk Management (ERM) Program for identifying, assessing, and managing risks and opportunities to effectuate the achievement of the University's goals and objectives. The ERM Program should be a formal and continuous process involving all programmatic and functional areas of the University. The University maintains a systematic organization-wide approach for identifying, assessing, and managing risks and opportunities that affect the University's ability to meet its strategic, operational, and financial goals and objectives; preserve its reputation for excellence; and protect its students, employees, and visitors. To meet these objectives, the University will develop and maintain an ERM Program that is intended to incorporate risk management efforts at all levels of the organization (SUNY, 2019).

With respect to the elements of the University's ERM Program, they include (SUNY, 2019):

- Leveraging and consolidating the existing internal control and compliance programs' structure, tools and information.
- Establishing an Enterprise Risk Management Committee which will be co-chaired by two members of the Chancellor's Executive Leadership Team, who will act jointly as the Chief Risk Officers for the University.
- A director of risk management, an internal control officer, and a compliance officer at System Administration to coordinate risk management activities throughout the University.
- Campus-based risk managers, internal control officers and coordinators, and compliance officers and/or coordinators at each campus (positions may be shared by one or more employees).
- Ongoing monitoring of internal and external audit reports and findings on financial management practices and other matters to consider and incorporate in risk management activities.
- Risk management activities to identify and assess the University's risks and opportunities using a framework that may include control environment, risk assessment, control activities, information and communication, and monitoring activities.
- Identifying and developing a strategic risk management profile and plans to manage strategic and enterprise level risks.
- Information and communication on risk management activities, including the sharing of best practices to help mitigate risk.
- Risk management training throughout the University system.
- Utilizing outside expertise for high-level consultation on industry trends, as well as the development and direction of key elements and documentation of the ERM Program.
- Reporting to the Audit Committee of the Board of Trustees on ERM activities.

SUNY refers to New York State Government components and principles of Internal Control. Indeed, the Office of the New York State Controller (2016) states that the five components of internal control must be successfully designed, implemented, and functioning sufficiently in order for the internal control system to be effective. The seventeen principles represent the fundamental concepts which are associated with specific components within the system. All components and principles are relevant in establishing an effective internal control system. An organization that has a strong system of internal control exhibits the following actions.

TABLE 2
FIVE COMPONENTS OF INTERNAL CONTROL

Control Environment
1. Demonstrates commitment to integrity and ethical values
2. Exercises oversight responsibility
3. Establishes structure, authority and responsibility
4. Demonstrates commitment to competence
5. Enforces accountability
Risk Assessment
6. Specifies suitable objectives
7. Identifies and analyzes risk
8. Assesses fraud risk
9. Manages risk during change
Control Activities
10. Selects and develops control activities
11. Selects and develops general controls over technology
12. Deploys controls through policies and procedures
Information and Communication
13. Uses relevant information
14. Communicates internally
15. Communicates externally
Monitoring
16. Conducts ongoing and/or separate evaluations
17. Evaluates and communicates deficiencies

Source: Office of the New York State Controller (2016)

We propose to explore more deeply the seventeen standards outlined in the table above by referring to the source. More focus is made in this paper on risk assessment. Risk can be identified into the following classes (Rejda & others, 2020):

- Pure and speculative risk: Pure risk is defined as a situation in which there are only the possibilities of loss or no loss. The only possible outcomes are adverse (loss) and neutral (no loss). Examples of pure risks include premature death, job-related accidents, catastrophic medical expenses, and damage to property from fire, lightning, flood, or earthquake. In contrast, speculative risk is defined as a situation in which either profit or loss is possible. For instance, if you purchase 100 shares of common stock, you would profit if the price of the stock increases but would lose if the price declines.
- Diversifiable Risk and Non-diversifiable Risk: Diversifiable risk is a risk that affects only individuals or small groups and not the entire economy. It is a risk that can be reduced or eliminated by diversification. For example, a diversified portfolio of stocks, bonds, and certificates of deposit (CDs) is less risky than a portfolio that is 100 percent invested in common stocks. In contrast, non-diversifiable is a risk that affects the entire economy or large numbers of persons or groups within the economy. It is a risk that cannot be eliminated or reduced by diversification. Examples include rapid inflation, cyclical unemployment, war, hurricanes, floods, and earthquakes because large numbers of individuals or groups are affected.

- Enterprise Risk is a term that encompasses all major risks faced by a business firm. Such risks include pure risk, speculative risk, strategic risk, operational risk, and financial risk. Strategic risk refers to uncertainty regarding the organization's financial goals and objectives; for example, if a university enters a new line of business, the line may be unprofitable. Operational risk results from the organization's business operations. For example, a colelge offers online programs may incur losses if "hackers" break into the college's computer. Enterprise risk also includes financial risk, which is becoming more essential in a commercial risk management program. Financial risk refers to the uncertainty of loss because of adverse changes in commodity prices, interest rates, foreign exchange rates, and the value of money. ERM combines into a single unified treatment program all major risks faced by the organization. By packaging major risks into a single program, the organization can offset one risk against another. Consequently, overall risk can be reduced.

The university top management first needs to identify all business objectives of its programs and units, including operational goals, reporting, and compliance requirements. These objectives should be specific enough to provide direction for managing the university's functions and should be stated in terms that reflect the responsibilities of its subunits.

After identifying all the university objectives, top management should coordinate with major stakeholders to identify all the risks associated with each objective (i.e., the events that would threaten the accomplishment of each objective). These risks can be both internal (e.g., human error, fraud, system breakdowns) and external (e.g., changes in legislation, natural disasters). It is essential that managers within the organization identify the risks associated with their respective objectives. There are many ways to look at risks, and no one can identify all potential risks. One recognized approach is to conduct a group brainstorming session with staff to generate ideas on what could go wrong in an organization, operation, or unit. It's a dynamic process, allowing you to consider how potential events might affect the achievement of your objectives Office of the New York State Comptroller (2019).

The following chart illustrates some of the places where the university can be exposed to risk, although it is not reflective of all potential risks.

FIGURE 5
POTENTIAL RISK EXPOSURE

Source: Office of the New York State Comptroller (2019)

In this regard, among the questions top management should consider are:

- How does the new technology contribute to achieving the university's mission?
- Does the new technology increase risks that may hinder the accomplishment of objectives?
- What changes to internal controls (e.g., control activities) are necessary to manage these risks?

The executive management should provide clear guidance to managers throughout the university to help them assess both the level and the nature of risks that and distinguish acceptable from unacceptable risks. Deans and other managers should use this guidance, along with the results of the organization's specific risk assessments, to determine actions necessary to manage each risk to an acceptable level. In each case, managers must decide whether to accept, reduce, transfer or avoid each risk entirely. For instance, in deciding how to manage the risk that unauthorized persons could gain access to the university electronic files, managers should consider the following possibilities:

- Accept the risk: Do not establish control activities - Management may choose to accept the risk of unauthorized access because consequences of such access are insignificant. (E.g., the files may not contain data that is sensitive.). Management might also choose to accept the risk if the cost of the associated control activities is greater than the cost of the unfavorable event.
- Reduce the risk: Establish control activities - Management cannot accept the current level of risk of unauthorized access because the files contain confidential or otherwise inherently valuable data. Therefore, management establishes control activities that are intended to reduce the risk of unauthorized access to an acceptable level. However, the risk is reduced only as long as the control activities function as intended.
- Transfer or share the risk - Management may decide to maintain electronic data in a vendor-operated cloud environment or an external data center operated by a business partner. Contract provisions may then allow management to transfer responsibility for all or part of the risk of improper access to the service provider or business partner.

- Avoid the risk: Do not carry out the function - Management determines that it cannot tolerate any risk of unauthorized access to the files or cannot adequately control such access. For instance, a file may contain extremely sensitive data, or access controls may not be feasible. In this case, management may decide that the impact of any unauthorized access to this file would be too risky or that access is too difficult or too costly to control. Therefore, management decides not to carry out this function (Office of the New York State Comptroller (2019).

In total, while many executives have essential responsibilities for ERM, including the Chief Risk Officer, Chief Financial Officer, Chief Legal Officer and Chief Audit Executive, the ERM process works best when all key managers and stakeholders of the university contribute. In other words, everyone in the university has some responsibility for enterprise risk management. The chief executive officer is ultimately responsible and should assume ownership. Other managers support the entity's risk management philosophy, promote compliance with its risk appetite, and manage risks within their spheres of responsibility consistent with risk tolerances. A risk officer, financial officer, internal auditor, and others often have key support responsibilities. Other entity personnel are responsible for executing enterprise risk management in harmony with established directives and protocols. The board of directors should provide important oversight to enterprise risk management and should be aware of and concurs with the entity's risk appetite. A number of external parties, such as customers, vendors, business partners, external auditors, regulators, and financial analysts often provide information useful in effecting enterprise risk management, but they are not responsible for the effectiveness of, nor are they a part of, the entity's enterprise risk management (COSCO, 2004).

In this context, the University Rector or President 's effective participation is important in terms of keeping the focus at a strategic level. The Rector or the President wants to know the answers to such questions as (DeLoach, 2014):

- What is it that we don't know that could erode or cause irreparable harm to the university's reputation and brand image?
- What are the soft spots in our strategic plan that could result in failure to deliver the expected strategic and financial results?
- What are the critical assumptions underlying the university strategy over the planning horizon? Is top management monitoring the external environment for changes that could render one or more of those assumptions invalid?
- If the university was to lose a key component of the supply chain (e.g.; Governmental funding; Ministry of Higher Education Ministry Support; Private sector financing), would the university be able to continue operations? If not, how long would it take to recover?
- Are there any unknown exposures to events that can abruptly shift the university's agenda to "damage control" in a heartbeat should they occur?
- If such exposures exist, what can be done cost effectively to prevent these potential future events from happening, and how will the university respond should the events occur?
- Based on the answers to the above questions, what does top management do differently going forward?

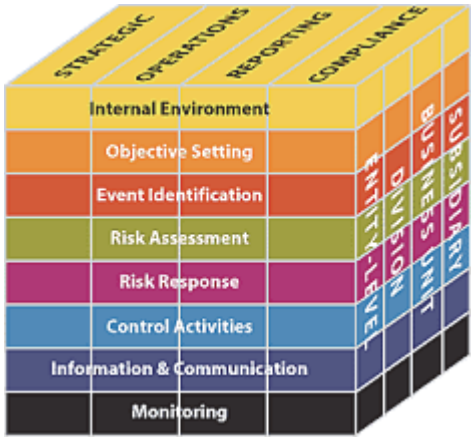
ERM provides the University's President with answers to these and other questions, if he or she is sufficiently involved to ensure the process is appropriately focused on the strategic and reputation risks that matter. In sum, support from the top is essential to an effectively functioning ERM process (DeLoach, 2014).

Determining whether an entity's enterprise risk management is "effective" is a judgment resulting from an assessment of whether the eight components are present and functioning effectively namely: Internal environment; Objective setting; Event identification; Risk assessment; Risk response; Control activities; Information & communication; & Monitoring. These eight components are also criteria for effective enterprise risk management. For the components to be present and functioning properly there should be no material weaknesses, and risk needs to have been brought within the entity's risk appetite. An

effective implementation of ERM assists the University in terms of achieving each of its four categories of objectives (COSO, 2004):

- Strategic – high-level goals, aligned with and supporting its mission
- Operations – effective and efficient use of its resources
- Reporting – reliability of reporting
- Compliance – compliance with applicable laws and regulations

FIGURE 6
FOUR CATEGORIES OF OBJECTIVES



Source: COSO (2004)

Integrating with strategy and performance, ERM provides a framework for boards and management in universities of all sizes. It builds on the current level of risk management that exists in the normal course of business. Moreover, it demonstrates how integrating enterprise risk management practices throughout the university helps to accelerate growth and enhance performance. It also contains principles that can be applied—from strategic decision-making through to performance. Additionally, enterprise risk management enriches management dialogue by adding perspective to the strengths and weaknesses of a strategy as conditions change, and to how well a strategy fits with the university's mission and vision. It allows managers to feel more confident that they've examined alternative strategies and considered the input of those in their university who will implement the strategy selected (COSO, 2017).

That said and done, it is proposed to discuss now the importance of internal control and risk management. Indeed, while the University President is responsible for ensuring an adequate internal control system is in place, the operation and monitoring of the system of internal control should be undertaken by individuals who collectively possess the necessary skills, technical knowledge, objectivity, and understanding of the university mission, vision, and strategic goals. In this context, the internal control or risk management function is responsible for identifying and inventorying risks to the mission of the university a unit and entity-wide basis. While monitoring these risks and continually reviewing the organization's environment for changes that could impact its mission is an ongoing process, a formal assessment of all inherently high-risk functions should occur at least annually, and lower risk categories should be reviewed at least every three years. The formal report of deficiencies should be directed to the University President and the audit committees. Moreover, the Internal Control Officer -or in some universities, the Chief Risk Officer - should present enterprise risks based on analysis of reported deficiencies and appropriate review of the internal and external environmental monitoring (SUNY, 2019).

The New York State Government Accountability, Audit and Internal Control Act (Act) requires that all state agencies institute a formal internal control program. In order to meet the requirements specified in the Act, the University and its campuses should include the following elements within its internal control program (SUNY, 2019):

Establish and Maintain Guidelines for a System of Internal Controls.

Internal control guidelines communicate an organization's management and programmatic objectives to its employees and provide the methods and procedures used to assess the effectiveness of its internal controls in supporting those objectives. According to the Division of Budget (DOB) Budget Policy and Reporting Manual Item B-350, internal control guidelines should:

- State the agency's support for internal controls and for providing staff with an understanding of the benefits of effective controls.
- Identify the agency's primary responsibilities and objectives
- Explain how internal controls are organized and managed;
- Define responsibilities of agency management, supervisors and staff
- Acknowledge that internal controls adhere to accepted standards; and
- Describe the organization's process for evaluating internal controls.
- Incorporate the guidance provided herein to assist the university campuses/colleges to adhere to the DOB directive.

Establish and Maintain a System of Internal Controls and a Program of Internal Control Review.

The system of internal control should be developed using the COSO (Committee of Sponsoring Organizations of the Treadway Commission) conceptual framework adopted in the Standards for Internal Controls in New York State Government, and should incorporate COSO's five components of internal control (See Appendix B for a detailed outline of these five elements). At minimum, the University's recommended general approach to the evaluation and improvement process should:

- Identify and clearly document the primary operating responsibilities (functions) of the campus. These responsibilities will be prescribed by the University and should be reinforced by senior management at the campus level.
- Define the objectives of these functions so they are easily understood by staff accountable for carrying out the functions. Managers should ensure that these objectives are documented for their respective function. The functional objectives should be used in developing the job responsibilities for each staff member within the functional unit.
- Identify and document the policies and procedures used to execute functions. The policies and procedures should be formalized, documented, and available to all appropriate staff members. Management should periodically review these policies and procedures and update them as necessary to reflect current operations.
- Identify the major functions of each of the campus' assessable units. These assessable units will be the basis for conducting risk assessments and internal control reviews.
- Include a process and cycle used to assess risk and test controls for the major functions. As a result of the risk assessment, each assessable unit should be categorized as high, medium or low risk. Internal control reviews must be conducted on all areas pre-determined by System Administration to be high risk over a three-year recurring cycle. Additional areas determined by the campus to be high risk should also be included in this review cycle. To assist campuses in conducting internal control reviews, checklists and tools are available on the university website. Management should conduct these reviews for their respective areas in conjunction with the internal control officer/coordinator.
- Assess the risks and consequences associated with controls failing to promote the objectives of major functions. Management, in conjunction with the internal control officer/coordinator, should determine the significance level assigned to each risk identified and how it relates in calculating the overall risk level of the unit/function.
- Test internal controls to ensure they are working as intended. In-depth internal control reviews are designed to test the control activities in place to help mitigate risks. The tools and checklists available to campuses have been developed using the COSO internal control

framework, as well as the Manager's Testing Guide published by the New York State Division of Budget.

- Institute a centrally monitored process to document, monitor and report deficiencies and corrective actions. The internal control officer/coordinator should facilitate and oversee all risk assessments and internal control reviews. All results should be documented and recorded by the internal control officer. Any control deficiencies noted should be communicated in swiftly by the internal control officer to management. Corrective action plans should be established by management to address these deficiencies. The implementation of corrective actions should be monitored by the internal control officer.

Make Available to Each Employee a Clear and Concise Statement of the University's/Campus's Generally Applicable Management Policies and Standards

All employees are expected to comply, along with detailed policies and procedures in completing their work. In this regard, all existing employees and all new hires should be familiar with applicable Federal, State, University, and campus policies and procedures. In order to communicate this effectively to all employees, a memorandum or "tone at the top" letter from the campus president should emphasize the importance of having good internal controls and assigning the responsibility for such upon each officer and employee. The memorandum or letter should refer the campus community to a campus website and/or include an informational brochure.

Designate an internal control officer at the University and campus levels to implement and review the University's/campuses' Internal Control Programs. The University and each of its affected campuses are required to designate an internal control officer. Based upon the internal control officer's other responsibilities, it may be necessary to delegate certain operational aspects of the campus' internal control program to designated staff (such as an internal control coordinator).

Implement Education and Training Efforts to Ensure Employee Awareness and Understanding of Internal Control Standards and Evaluation Techniques.

Campuses should identify staff requiring internal control training and the depth and content of that training. The education and training efforts should be ongoing and may vary depending upon the degree of responsibilities of the employee. Specific courses should be directed at line staff, middle managers and executive management. For campuses with internal audit functions, training and education should be offered on the appropriate role of the auditor within the campus' internal control program.

Periodically Evaluate the Need for an Internal Audit Function.

Under DOB Budget Policy and Reporting Manual Item B-350, the University is required to maintain an internal audit function. The function is required to be maintained in conformance with internal audit standards promulgated by the Institute of Internal Auditors in their International Standards for the Professional Practice of Internal Auditing (IIA Standards, 2019). The decisions to establish and maintain internal audit functions at the campuses are the prerogative of the campus presidents, although consultations with the University Auditor for such a need are encouraged. Adherence to the auditing standards noted above is also required of campus-based auditors.

Reporting

On or before April 30th the University is required by DOB Budget Policy and Reporting Manual Item B-350 to certify compliance with the provisions of the Act as outlined in the preceding sections of these guidelines, as well as any subsequent directives established by DOB. The Chancellor signs the annual certification on behalf of the University, which is based upon an evaluation of the internal control activities present for the state fiscal year ended March 31st. As part of this process, the University requests that the presidents of State-operated campuses, chief administrative officers of contract colleges, and System Administration also affirm compliance with provisions of the Act, or where such affirmation is not possible, submit a corrective action plan to achieve compliance as soon as practical. Self-assessment tools

have been made available to all campuses to assist in the evaluation of compliance. Compliance activities may also be the subject of an internal or external audit.

The University, as part of its responsibilities for monitoring the internal control program, also requires all campuses to report annually in conjunction with their certification the status of specific, significant internal control activities, testing, and resolution of findings contained in pertinent audits of University/campus activities or programs. Important deficiencies identified during internal control reviews should be noted, as well as actions taken (or planned) to address these deficiencies. The University is responsible for monitoring each college or campus' noted deficiencies and will assess whether significant weaknesses are adequately addressed in subsequent reporting periods. The University's internal control officer or coordinator submits the forms provided for the annual status report.

In addition to the Act, the Office of the State Comptroller (OSC) requires the head of each state agency (e.g. Commissioner, Chancellor, Executive Director), or their designee, to submit a certification to the Comptroller annually that the agency has sufficient internal controls in place for various aspects of the procurement process. OSC will specify which segments will require certification for the given year.

One should keep in mind though that the effectiveness of this internal control system depends on the following elements:

- The system of internal control should be embedded in the operations of the university and form part of its culture.
- Controls should be capable of responding quickly to evolving risks, both internal and external.
- The costs of internal controls must be balanced against the benefits, including the risks they are designed to manage.
- The system of internal control must include procedures for reporting immediately to appropriate levels of management any significant control failings or weaknesses that are identified, together with details of the corrective action being undertaken.
- Controls can help minimize the occurrence of errors and breakdowns but cannot provide absolute assurance that they will not occur.

CONCLUSION

ERM as implemented by SUNY is just a suggestion and evidently other international universities can be used as a benchmark by Saudi universities. We recognize that Saudi universities should adjust ERM in line with the national cultural characteristics, the organizational strategic goals, and the national requirements. Nevertheless, any risk management strategy should integrate a variety of risks including strategic, financial, operational, and compliance. Once the top management of the university is convinced about the utility of ERM, an orientation session prior to the interviews, questionnaires, and voting workshop is critical for faculty and staff to understand ERM concepts and think more deliberately about the risks they may be facing. In this regard, efficient scheduling of the orientation and workshop is critical to a smooth implementation. Initial implementation workshops need to be scheduled during the academic year if faculty, staff and students are going to be included in the process. Mid-semester seems to work best.

To allow for good discussion in the workshop, no more than twenty five people should be involved. Moreover, splitting the voting workshops into two half-day sessions is a more effective use of staff time. Workshop participants weary of the voting process if this is conducted in one eight-hour timeframe. Furthermore, feedback of workshop results to campus participants should be completed within a one-month timeframe. To keep risk lists and heat maps current the Core Working Group estimates should be updated every 18-24 months through a follow up risk assessment and validation session University of Wisconsin System. (2019).

In total, ERM should support better structure, reporting, and analysis of risks. Standardized reports that track enterprise risks can improve the focus of directors and executives by providing data that enables better risk mitigation decisions. The variety of data (status of key risk indicators, mitigation strategies, new

and emerging risks, etc.) helps leadership understand the most important risk areas. These reports can also help leaders develop a better understanding of risk appetite, risk thresholds, and risk tolerances. One of the major values of ERM risk reporting is improved, timeliness, conciseness, and flexibility of the risk data. This provides the data needed for improved decision-making capabilities within the executive and director levels, and in other layers of management. ERM helps management recognize and unlock synergies by aggregating and sharing all corporate risk data and factors and evaluating them in a consolidated format.

Despite its benefits, enterprise risk management has limitations. Indeed, drawbacks result from the realities that human judgment in decision making can be faulty, decisions on responding to risk and establishing controls need to consider the relative costs and benefits, breakdowns can occur because of human failures such as simple errors or mistakes, controls can be circumvented by collusion of two or more people, and management has the ability to override enterprise risk management decisions. These limitations preclude a board and management from having absolute assurance as to achievement of the entity's objectives.

REFERENCES

Agarwal, R., & Virine, L. (2019). Integration Stages of Project Risk Management (PRM) into Enterprise Risk Management (ERM). *International Journal of Risk and Contingency Management*, 8(1), 13-33.

Alzharani, A.M., & Aljaaidi, K.S. (2015). An empirical investigation of audit committee effectiveness and risk management: Evidence from Saudi Arabia. *Accounting & Taxation*, 7(1), 39-49.

Arena, M., Azzone, G., Cagno, E., Ferretti, G., Prunotto, E., Silvestri, A., & Trucco, P. (2013). Integrated risk management through dynamic capabilities within project-based organizations: The company dynamic response map. *Risk Management*, 15(1), 50-77.

Association of Government Accountants (AGA). (2019). http://www.agacgfm.org

Banham, R. (2011). ERM IN ACTION. *Business Insurance*, 45(5), 9. Retrieved from http://ezproxy.library.usyd.edu.au/login?url=https:/ /search-proquestcom.ezproxy1.library.usyd.edu.au/docview/851207580?accountid=14757

Beasley. M.S. (2016). *What is ERM. NC State University*. Deloitte Professor of ERM and Director of the ERM Initiative North Carolina State University

Beringer, C., Jonas, D., & Kock, A. (2013). Behavior of internal stakeholders in project portfolio management and its impact on success. *International Journal of Project Management*, 31(6), 830-846.

Boukhari, M. (2013). *Enterprise risk management application implementation case study*. Paper presented at PMI® Global Congress 2013—EMEA, Istanbul, Turkey. Newtown Square, PA: Project Management Institute.

Boyd, D. A. (2010). Real-world risk management strategies for physician practices. *Journal of Healthcare Risk Management*, 29(3), 49-50.

Bugalla, J., & Narvaez, K. (2011). *ERM and project management*. New York: Risk and Insurance Management Society, Inc.

Carvalho, M. M. D., & Junior, R. R. (2015). Impact of risk management on project performance: The importance of soft skills. *International Journal of Production Research*, 53(2), 321-340.

Chapman, R. J. (2011). *Simple tools and techniques for enterprise risk management,* (2nd ed.). GB: John Wiley & Sons Inc.

COSO. (2004). Enterprise risk management-integrated framework. Committee of Sponsoring Organizations of the Treadway Commission. New York. Retrieved from https://www.coso.org/Documents/COSO-ERMExecutive-Summary.pdf

COSO. (2004). Enterprise Risk Management — Integrated Framework. Executive Summary. COSO.org website.

COSO. (2004). Enterprise Risk Management - Integrated Framework: Executive Summary & Framework, Committee of Sponsoring Organizations of the Treadway Commission, Jersey City, NJ.

COSO. (2017). Committee of Sponsoring Organizations of the Treadway Commission. Enterprise Risk Management Integrating with Strategy and Performance. Executive summary. Retrieved from https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf

Curtis, P., & Carey, M. (2012). *Risk assessment in practice*. COSO. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Governance-Risk-Compliance/dttl-grc-riskassessmentinpractice.pdf

Dabari, I.J., & Saidin, S.Z. (2016). A moderating role of board characteristics on enterprise risk management implementation: Evidence from the Nigerian Banking Sector. *International Journal of Economics and Financial Issues*, 6(4), 96-103.

DeLoach, J. (2014). *The Role of Executive Management in ERM*. Corporate Compliance Insights. Discussion of ERM plan implementation is based on "5 Tips for Successful ERM Implementation," Michael Goni, http://www.ssapchat.com, March 7, 2018; "10 Easy Steps to Implement Enterprise Risk Management," Carol Fox, Risk Management, November 2014, and "Implementing Enterprise Risk Management: Getting the Fundamentals Right," Jerry Miccolis, http://www.IRMI.COM

Do, H., Railwaywalla, M., & Thayer, J. (2016). *Integration of ERM with Strategy. Case Study Analysis*. Poole College of Management, NCSU.

Frigo, M.L., & Anderson, R.J. (2014). Risk management framework: adapt, don't adopt. *Strategic Finance*, 96, 47-51.

Gates, S., Nicolas, J.L., & Walker, P.L (2012). Enterprise risk management: A process for enhanced management and improved performance. *Management Accounting Quarterly*,13(3), 28-38. Retrieved from https://www.researchgate.net/publication/282063906_Enterprise_Risk_Management_A_Process_for_Enhanced_Management_and_Improved_Performance

Gong, W., Liu, J. Y., & Zou, P. X. W. (2013). Managing project risk at the enterprise level: Exploratory case studies in China. *Journal of Construction Engineering and Management*, 139(9), 1268-1274.

Guidance on Control. (2019). The Canadian Institute of Chartered Accountants (COCO). Retrieved from http://www.cica.ca

Hillson, D. (2006). *Integrated risk management as a framework for organisational success*. Paper presented at PMI® Global Congress 2006—North America, Seattle, WA. Newtown Square, PA: Project Management Institute. http://www.osc.state.ny.us/agencies/guide/MyWebHelp/Content/XII/4/D.htm

Institute of Internal Auditors (IIA). (2019). http://www.theiia.org

Internal Control - Integrated Framework (COSO). (2019). Retrieved from http://www.coso.org/documents/990025P_Executive_Summary_final_may20_e.pdf

ISACA. (2019). Control Objectives for Information and Related Technology (COBIT). Retrieved from http://www.isaca.org/COBIT

Jonas, V. (2011). *Portfolio risk management: Aligning projects with business objectives to deliver value*. PMI Global Congress 2011, Dublin Ireland.

Jordan, S., Jørgensen, L., & Mitterhofer, H. (2013). Performing risk and the project: Risk maps as mediating instruments. *Management Accounting Research*, 24(2), 156-174.

Kreiser. J. (2013). *Five Benefits of Enterprise Risk Management*. Retrieved from https://www.claconnect.com/resources/articles/five-benefits-of-enterprise-risk-management

Liebenberg, A. P., & Hoyt, R. E. (2003). The determinants of enterprise risk management: Evidence from the appointment of chief risk officers. *Risk Management and Insurance Review*, 6(1), 37-52.

Muralidhar, K. (2010). Enterprise risk management in the Middle East oil industry: An empirical investigation across GCC countries. *International Journal of Energy Sector Management*, 4(1), 59-86

New York State Division of the Budget. (2019.) Budget Policy & Reporting Manual – Item B-350 Governmental Internal Control and Internal Audit Requirements http://www.budget.ny.gov/guide/bprm/b/b350.html
New York State Guide to Financial Operation. (2019). Section XI.11.F - Contract Monitoring http://www.osc.state.ny.us/agencies/guide/MyWebHelp/Content/XI/11/F.htm
New York State Guide to Financial Operation. (2019). Section XII.4.D - Certification of Internal Controls over the Payment Process
New York State Internal Control Act. (2019). Retrieved from http://www.osc.state.ny.us/agencies/ictf/docs/Internal%20Control%20Act.pdf?cl=39&a=73
New York State Internal Control Association (NYSICA). (2019). http://www.nysica.com
New York State Internal Control Task Force Report. (2006). New York State Internal Control Act Implementation Guide: Strengthening Compliance with the Act and Standards. Retrieved from http://www.osc.state.ny.us/agencies/ictf/docs/implement_guide_20060907.pdf
New York State Office of Information Technology Services. (2019). Retrieved from http://www.its.ny.gov/
Office of Management and Budget. (2019). OMB A-123 Management Accountability and Control. Retrieved from http://www.whitehouse.gov/omb/circulars/a123/a123.html
Office of the New York State Controller State Comptroller. (2016). Standards for Internal Control in New York State Government. Retrieved from https://www.osc.state.ny.us/
Public Company Accounting Oversight Board (PCAOB). (2019). http://www.pcaobus.org/
Rao, A., & Marie, A. (2007). Current practices of enterprise risk management in Dubai: A survey of managers and executives from more than 100 businesses in Dubai, UAE. *Management Accounting Quarterly*, 8(3), 10-22.
SUNY. (2014). Internal Control Program. Retrieved from https://www.suny.edu/sunypp/documents.cfm?doc_id=289&CFID=4136478&CFTOKEN=a26f2c186194542d-31A40CB4-F7B5-8387-D7A016170FA16E52#appendicies
The Institute for Internal Auditor Standards- IIA. (2019). International Standards for the Professional Practice of Internal Auditing (Standards). Retrieved from https://na.theiia.org/standards-guidance/mandatory-guidance/Pages/Standards.aspx
The National Institute for Standards and Technology (NIST). (2019). Special Publications Library. Retrieved from http://csrc.nist.gov/publications/PubsSPs.html
The University of Washington. (2019). Proposed Application of the Enterprise Risk Management Concept at the University of Washington. Retrieved from https://finance.uw.edu/sites/default/files/erm/proposed-application-of-erm-at-the-UW.pdf
U.S. Government Accountability Office. (2019). Internal Control Management and Evaluation Tool. Retrieved from http://www.gao.gov/new.items/d011008g.pdf
U.S. Government Accountability Office. (2019). Standards for Internal Control in the Federal Government. Retrieved from http://www.gao.gov/products/GAO-14-704G
University of California. (2019). Office of the President. Enterprise Risk and Resilience. Retrieved from https://www.ucop.edu/enterprise-risk-and-resilience/erm/index.html
University of Maryland Baltimore. (2019). Enterprise Risk Management. Retrieved from https://www.umaryland.edu/about-umb/offices/operations-and-planning/enterprise-risk-management/
University of Wisconsin System. (2019). Enterprise Risk Management. Lessons learned. Retrieved from https://www.wisconsin.edu/risk-management/enterprise-risk-management/#achievements-and-lessons-learned
University of Wisconsin System. (2019). Enterprise Risk Management Handbook. Retrieved from https://www.wisconsin.edu/risk-management/download/ERM_Handbook(2).pdf
Vrhovec, S. L. R., Hovelja, T., Vavpotič, D., & Krisper, M. (2015). Diagnosing organizational risks in software projects: Stakeholder resistance. *International Journal of Project* Management, 33(6), 1262-1273.

Yin, R. K. (1984). *Case study research: Design and methods*. Beverly Hills, Calif: Sage Publications.
Zhao, X., Hwang, B., & Low, S. P. (2015). Enterprise risk management in international construction firms: Drivers and hindrances. *Engineering, Construction and Architectural Management*, 22(3), 347-366.