COSO Internal Control Integrated Framework
Risk Assessment and Control Activities

One Day Course

City University of New York

April 17, 2019

Presented by:

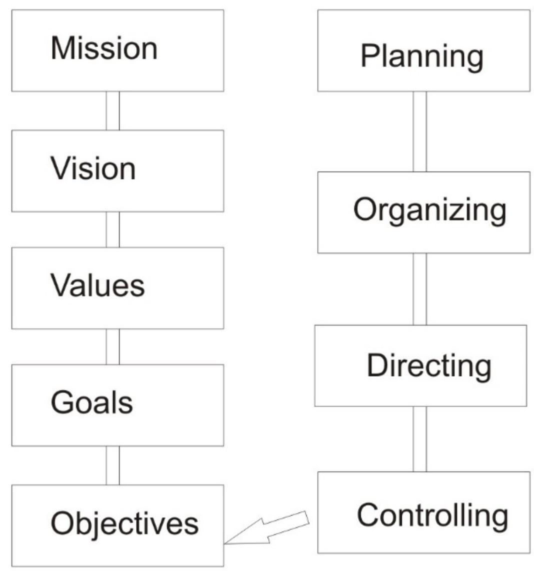
Michael L. Piazza
Principal Associate
Professional Development Associates

www.pda-usa.com

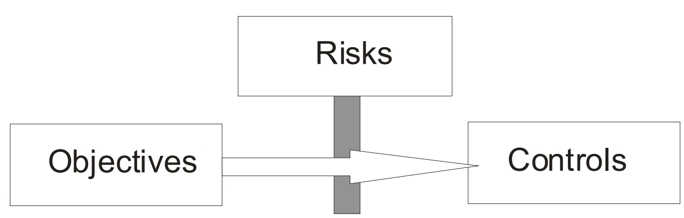
COSO Integrated Framework of Internal Control
Risk Assessment and Control Activities
April 17, 2019

9:00 - 10:15	*Course Overview and Introductions*
10:15 - 10:30	*Break*
10:30 - 10:45	*The Summary and Definitions of the COSO Framework and the Risk Assessment and Control Activities Components:* An overview of the COSO Framework and the attributes comprising the risk assessment and control activities components are explored, including the management function and the role of controls in mitigating risk and accomplishing objectives.
10:45 - 11:00	*Objectives Setting and Internal Control:* A precondition to risk assessment is the establishment of objectives, linked at different levels of the entity. The COSO Objectives Setting section is explored.
11:00 - 11:30	*Specifies Suitable Objectives: Principle 6*
11:30 - 12:00	*Identifies and Analyzes Risk: Principle 7*
12:00 - 1:00	*Luncheon*
1:00 - 2:15	*Assesses Fraud Risk: Principle 8*
2:15 - 2:45	*Identifies and Analyzes Significant Change: Principle 9*
2:45 - 3:00	*Break*
3:00 - 3:30	*Selects and Develops Control Activities: Principle 10*
3:30 - 3:45	*Selects and Develops General Controls over Technology: Principle 11*
3:45 - 4:15	*Deploys through Policies and Procedures: Principle 12*
4:00 - 4:30	*Summary, Discussion and Conclusion:* The concepts and applications from the day are reviewed to summarize the Internal Control Integrated Framework risk assessment and control activities components. Participant objectives and challenges are addressed.

Organizational and Management Functions:



Objectives – Risks – Controls Relationships



Simply Defined:
Objectives – Things that an organization wants to accomplish

Risks – Those factors, internal or external, that can prevent an objective from being accomplished

Controls – Those activities (actions, policies, procedures, etc.) that help to ensure that an objective is accomplished and that risks are mitigated and otherwise minimized.

Governance Definitions

Governance: is that separate process or certain part of management or leadership processes that makes decisions that define expectations, grant power, or verify performance. Frequently a government is established to administer these processes and systems.

Governance (in business): is the action of developing and managing consistent, cohesive policies, processes and decision rights for a given area of responsibility. For example, managing at a corporate level: privacy, internal investment, the use of data.

Origin: The word derives from Latin origins that suggest the notion of 'steering'. This sense of 'steering' a group or society can be contrasted with the traditional 'top-down' approach of governments 'driving' society or the distinction between 'power to' in contrast to governments 'power over'.

General Description: As a process, governance may be carried out for any size organization from a single human being to all of humanity, and it may be carried out for any purpose, good or evil, for profit or not. A reasonable or rational purpose of governance is to see to it (assure), sometimes on behalf of others, that the organization produces a worthwhile pattern of good results while avoiding an undesirable pattern of bad circumstances.

Perhaps the most moral or natural purpose of governance is to assure, on behalf of those governed, a worthy pattern of good while avoiding a truly undesirable pattern of bad. The ideal purpose, obviously, would assure a perfect pattern of good with no bad. A government, then, is a set of inter-related positions that govern and use or exercise power, particularly coercive power.

Governance (IIA Glossary): The combination of processes and structures implemented by the board in order to inform, direct, manage, and monitor the activities of the organization toward the achievement of its objectives.

Uncertainty and Value

Uncertainty: Enterprises operate in environments where factors such as globalization, technology, regulation, restructurings, changing markets, and competition create uncertainty. Uncertainty emanates from an inability to precisely determine the likelihood that potential events will occur and the associated outcomes.

Value: Value is created, preserved or eroded by management decisions ranging from strategy setting to operating the enterprise day-to-day. Inherent in decisions is recognition of risk and opportunity, requiring that management1 considers information about internal and external environments, deploys precious resources and recalibrates enterprise activities to changing circumstances.

Realized Value: Entities realize value when stakeholders derive recognizable benefits that they in turn value. For companies, shareholders realize value when they recognize value creation from share-value growth. For governmental entities, value is realized when constituents recognize receipt of valued services at an acceptable cost. Stakeholders of not-for-profit entities realize value when they recognize receipt of valued social benefits. Enterprise risk management facilitates management’s ability to both create sustainable value and communicate the value created to stakeholders.

Limitations of Internal Control

Internal control, no matter how well designed, implemented and conducted, can provide only reasonable assurance to management and the board of directors of the achievement of an entity's objectives. The likelihood of achievement is affected by limitations inherent in all systems of internal control. These include the realities that human judgment in decision making can be faulty, external events outside the organization's control may arise, and breakdowns can occur because of human failures such as making errors. Additionally, controls can be circumvented by two or more people colluding, and because management can override the system of internal control.

Internal control has been viewed by some observers as ensuring that an entity will not fail—that is, the entity will always achieve its operations, reporting, and compliance objectives. In this sense, internal control sometimes is looked upon as a cure-all for all real and potential business ills. This view is misguided. Internal control is not a panacea.

In considering limitations of internal control, two distinct concepts must be recognized. The first set of limitations acknowledges that certain events or conditions are simply beyond management's control. The second acknowledges that no system of internal control will always do what it is designed to do. The best that can be expected in any system of internal control is that reasonable assurance be obtained, which is the focus of this chapter. Second, internal control cannot provide absolute assurance for any of the objective categories.

The first set of limitations acknowledges that certain events or conditions are simply outside management's control. The second acknowledges that no system of internal control will always do what it is designed to do. The best that can be expected in any of system of internal control is that reasonable assurance be obtained, which is the focus of this chapter.

Reasonable assurance does not imply that systems of internal control will frequently fail. Many factors, individually and collectively, serve to strengthen the concept of reasonable assurance. Controls that support multiple objectives or that effect multiple principles within or across components reduce the risk that an entity may not achieve its objectives. Furthermore, the normal, everyday operating activities and responsibilities of people functioning at various levels of an organization are directed at achieving the entity's objectives. Indeed, it is likely that these activities often apprise management about the process toward the entity's operations objectives, and also support the achievement of compliance and reporting objectives. However, because of the inherent limitations discussed here, there is no guarantee that, for example, an uncontrollable event, mistake, or improper incident could never occur. In other words, even an effective system of internal control may experience failures. Reasonable assurance is not absolute assurance.

Preconditions of Internal Control

The Framework specifies several areas that are part of the management process but not part of internal control. Two such areas relate to the governance process that extends the board's role beyond internal control and establishing objectives as a precondition to internal control. There is a dependency established on these areas, among others, to also be effective. For example, an entity's weak governance processes for selecting, developing, and evaluating board members may limit its ability to provide appropriate oversight of internal control. Similarly, ineffective strategy-setting or objective-setting processes would challenge the entity's ability to identify poorly specified, unrealistic, or unsuitable objectives. A system of internal control cannot encompass all activities undertaken by the entity, and weaknesses in these areas may impede the organization from having effective internal control.

Judgment

The effectiveness of internal control is limited by the realities of human frailty in the making of business decisions. Such decisions must be made with human judgment in the time available, based on information at hand, subject to management biases, and under the pressures of the conduct of business.

Some decisions based on human judgment may later, with the clarity of hindsight, be found to produce less than desirable results, and may need to be changed.

External Events
Internal control, even effective internal control, operates at different levels for different objectives. For objectives relating to the effectiveness and efficiency of an entity's operations—achieving its mission, value propositions (e.g., productivity, quality, and customer service), profitability goals, and the like—internal control cannot provide reasonable assurance of the achievement when external events may have a significant impact on the achievement of objectives and the impact cannot be mitigated to an acceptable level. In these situations, internal control can only provide reasonable assurance that the organization is aware of the entity's progress, or lack of it, toward achieving such objectives.

Management Override
Even an entity with an effective system of internal control may have a manager who is willing and able to override internal control. The term "management override" is used here to mean overruling prescribed policies or procedures for illegitimate purposes with the intent of personal gain or an enhanced presentation of an entity's performance or compliance. A manager of a division or operating unit, or a member of senior management, might override the control for many reasons such as to:

- Increase reported revenue to cover an unanticipated decrease in market share
- Enhance reported earnings to meet unrealistic budgets
- Boost the market value of the entity prior to a public offering or sale
- Meet sales or earnings projections to bolster bonus payouts tied to performance
- Appear to cover violations of debt covenant agreements
- Hide lack of compliance with legal requirements

Override practices include deliberately making misrepresentations to bankers, lawyers, accountants, and vendors, and intentionally issuing false documents such as purchase orders and sales invoices. Management override should not be confused with management intervention, which represents management's actions to depart from prescribed controls for legitimate purposes. Management intervention is necessary to deal with non-recurring and non-standard transactions or events that otherwise might be handled inappropriately. Provision for management intervention is necessary because no process can be designed to anticipate every risk and every condition. Management's actions to intervene are generally overt and subject to policies and procedures or otherwise disclosed to appropriate personnel. Actions to override usually are not documented or disclosed, and have the intent to cover up the actions.

Collusion
Collusion can result in internal control deficiencies. Individuals acting collectively to perpetrate and conceal an action from detection often can alter financial or other management information so that it cannot be detected or prevented by the system of internal control. Collusion can occur, for example, between an employee who performs controls and a customer, supplier, or another employee, Sales and/or operating unit management might collude to circumvent controls so that reported results meet budgets or incentive targets.

Objectives Setting and Internal Control

An organization adopts a mission and vision, sets strategies, establishes objectives it wants to achieve, and formulates plans for achieving them. Objectives may be set for an entity as a whole, or be targeted to specific activities within the entity. Though many objectives are specific to a particular entity, some are widely shared. For example, objectives common to most entities are sustaining organizational success, reporting to stakeholders, recruiting and retaining motivated and competent employees, achieving and maintaining a positive reputation, and complying with laws and regulations.

Supporting the organization in its efforts to achieve objectives are five components of internal control:

- **Control Environment**
- **Risk Assessment**
- **Control Activities**
- **Information and Communication**
- **Monitoring Activities**

Relationship of Objectives, Components, and the Entity:

A *direct* relationship exists between objectives, which are what an entity strives to achieve, components, which represent what is required to achieve the objectives, and entity structure (the operating units, legal entities, and other structures). The relationship can be depicted in the form of a cube.

- The three categories of objectives operations, reporting, and compliance are represented by the columns.

- The five components are represented by the rows.

- The entity structure, which represents the overall entity, divisions, subsidiaries, operating units, or functions, including business processes such as sales, purchasing, production, and marketing and to which internal control relates, are depicted by the third dimension of the cube.

Each component cuts across and applies to all three categories of objectives. For example, attracting, developing, and retaining competent people who are able to conduct internal control—part of the control environment component—is relevant to all three objectives categories.

The three categories of objectives are not parts or units of the entity. For instance, operations objectives relate to the efficiency and effectiveness of operations, not specific operating units or functions such as sales, marketing, procurement, or human resources.

Accordingly, when considering the category of objectives related to reporting, for example, knowledge of a wide array of information about the entity's operations is needed. In that case, focus is on the middle column of the model—reporting objectives—rather than on the operations objectives category.

Internal control is a dynamic, iterative, and integrated process. For example, risk assessment not only influences the control environment and control activities, but also may highlight a need to reconsider the entity's requirements for information and communication, or for its monitoring activities. Thus, internal control is not a linear process where one component affects only the next. It is an integrated process in which components can and will impact another.

No two entities will, or should, have the same system of internal control. Entities, objectives, and systems of internal control differ dramatically by industry and regulatory environment, as well as by internal considerations such as the size, nature of the management operating model, tolerance for risk, reliance on technology, and competence and number of personnel. Thus, while all entities require each of the components to maintain effective internal control over their activities, one entity's system of internal control usually looks different from another's.

Objectives

Management, with board oversight, sets entity-level objectives that align with the entity's mission, vision, and strategies. These high-level objectives reflect choices made by management and board of directors about how the organization seeks to create, preserve, and realize value for its stakeholders. Such objectives may focus on the entity's unique operations needs, or align with laws, rules, regulations, and standards imposed by legislators, regulators, and standard setters, or some combination of the two. Setting objectives is a prerequisite to internal control and a key part of the management process relating to strategic planning.

Individuals who are part of the system of internal control need to understand the overall strategies and objectives set by the organization. As part of internal control, management specifies suitable objectives so that risks to the achievement of such objectives can be identified and assessed. Specifying objectives includes the articulation of specific, measurable or observable, attainable, relevant, and time-bound objectives.

However there may be instances where an entity might not explicitly document an objective. Objectives specified in appropriate detail can be readily understood by the people who are working toward achieving them.

Categories of Objectives

The Framework groups entity objectives into the three categories of operations, reporting, and compliance.

Operations Objectives

Operations objectives relate to achievement of an entity's basic mission - the fundamental reason for its existence. These objectives vary based on management's choices relating to structure, industry considerations, and performance of the entity. Entity-level objectives cascade into related sub-objectives for operations within the divisions, subsidiaries, operating units, and functions, directed at enhancing effectiveness and efficiency in moving the entity toward its ultimate goal.

As such, operations objectives may relate to improving financial performance, productivity (e.g., avoiding waste and rework), quality, environmental practices, innovation, and customer and employee satisfaction. These objectives pertain to all types of entities. For example, a for-profit entity may focus on revenue, profitability, return on assets, and liquidity. In contrast, a not-for-profit entity, though certainly concerned with revenues or levels of spending, may focus more on increasing donor participation. A governmental agency may focus primarily on executing its spending in line with the designated purposes of its appropriators to ensure that the spending supports its mission objectives. If an entity's operations objectives are not well conceived or clearly specified, its resources may be misdirected.

Safeguarding of Assets

The operations category of objectives includes safeguarding of assets, which refers to protecting and preserving entity assets. For instance, an entity may set objectives relating to the prevention of loss of assets and the timely detection and reporting of any such losses. These objectives form the basis of assessing risk relating to safeguarding of assets and selecting and developing controls needed to mitigate such risk.

The efficient use of an entity's assets, and prevention of loss through waste, inefficiency, or poor business decisions (e.g., selling product at too low a price, extending credit to bad risks, failing to retain key employees, preventing patent infringement, incurring unforeseen liabilities) relate to a broader operations objectives and are not a specific consideration relating to safeguarding of assets.

Laws, rules, regulations, and standards have created an expectation that management reporting on internal control includes controls relating to preventing and detecting unauthorized acquisition, use, or disposition of the assets. In addition, some entities consider safeguarding of assets a separate category of objective, and that view can be accommodated within the application of the Framework.

Reporting Objectives

Reporting objectives pertain to the preparation of reports for use by organizations and stakeholders. Reporting objectives may relate to financial or non-financial reporting and to internal or external reporting. Internal reporting objectives are driven by internal requirements in response to a variety of potential needs such as the entity's strategic directions, operating plans, and performance metrics at various levels. External reporting objectives are driven primarily by regulations and/or standards established by regulators, and standard-setting bodies.

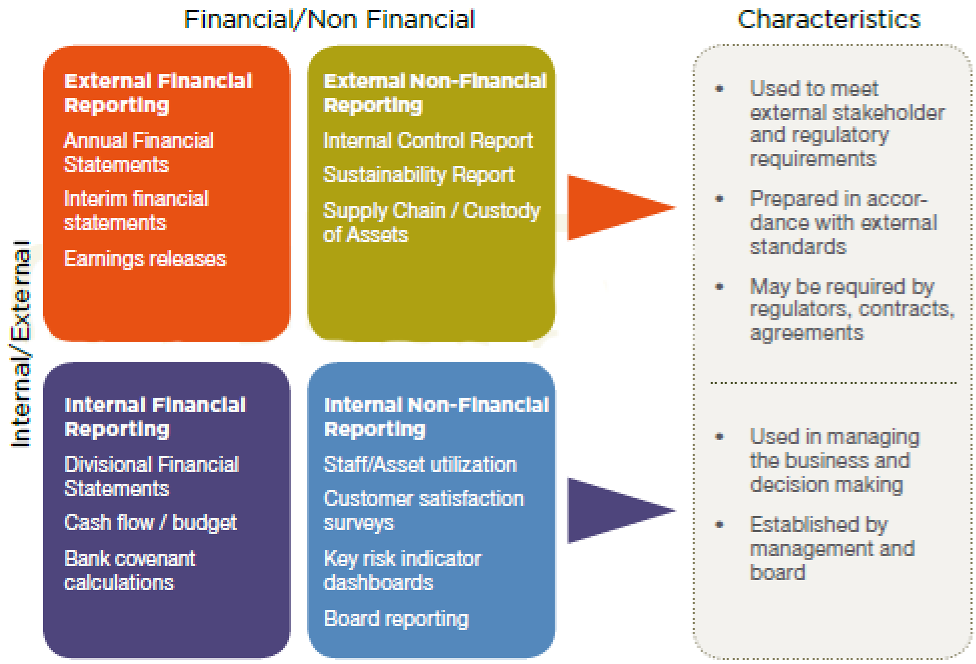
- External Financial Reporting Objectives - Entities need to achieve external financial reporting objectives to meet obligations to and expectations of stakeholders. Financial statements are necessary for accessing capital markets and may be critical to being awarded contracts or in dealing with suppliers and vendors. Investors, analysts, and creditors often rely on an entity's external financial statements to assess its performance against peers and alternative investments. Management may also be required to publish financial statements using objectives set forth by rules, regulations, and standards.

- External Non-Financial Reporting Objectives - Management may report external non-financial information in accordance with regulations, standards, or frameworks. An entity may engage an independent auditor to report on its conformance with standards published by standard-setting bodies. Nonfinancial reporting requirements as set forth by regulations and standards for management reporting on the effectiveness of internal control over financial reporting are part of external non-financial reporting objectives. For purposes of the Framework, external reporting in the absence of a regulation, standard, or framework represents external communication.

- Internal Financial and Non-Financial Reporting Objectives - Internal reporting to management and the board of directors includes information deemed necessary to manage the organization. It supports decision making and assessment of the entity's activities and performance. Internal reporting objectives are based on preferences and judgments of management and the board. Internal reporting objectives vary among entities because different organizations have different strategic directions, operating plans, and expectations.

Relationship within Reporting Category of Objective:

The overall relationship between the four sub-categories of reporting objectives is depicted in the graphic below.



Reporting objectives are different from the information and communication component of internal control. Management establishes, with board oversight, reporting objectives when the organization needs reasonable assurance of achieving a particular reporting objective. In these situations all five components of internal control are needed. For instance, in preparing internal non-financial reporting to the board on the status of merger integration efforts, the organization specifies internal reporting objectives (e.g., prepares reliable, relevant, and useful reports), assigns competent individuals, assesses risks relating to specified objectives, selects and develops controls within the five components necessary to mitigate such risks, and monitors components of internal control supporting the specified non-financial reporting objective.

In contrast, the Information and Communication component supports the functioning of all components of reporting objectives, as well as operations and compliance objectives. For instance, controls within information and communication support the preparation of the above report, helping to provide relevant and quality information underlying the report, but these controls are only part of the overall system of internal control.

Compliance Objectives

Entities must conduct activities, and often take specific actions, in accordance with applicable laws and regulations. As part of specifying compliance objectives, the organization needs to understand which laws, rules and regulations apply across the entity. Many laws and regulations are generally well known, such as those relating to human resources, taxation, and environmental compliance, but others may be more obscure, such as those that apply to an entity conducting operations in a remote foreign territory.

Laws and regulations establish minimum standards of conduct expected of the entity. The organization is expected to incorporate these standards into the objectives set for the entity. Some organizations will set objectives to a higher level of performance than established by laws and regulations. In setting those objectives, management is able to exercise discretion relative to the performance of the entity. For instance, a particular law may limit minors working outside school hours to eighteen hours in a school week. However, a retail food service company may choose to limit its minor-age staff to working fifteen hours per week.

For purposes of the Framework, compliance with an entity's internal policies and procedures, as opposed to compliance with external laws and regulations as discussed above, relates to operations objectives.

Overlap of Objectives Categories

An objective in one category may overlap or support an objective in another. For example, "closing financial reporting period within five workdays" may be a goal supporting primarily an operations objective-to support management in reviewing business performance. But it also supports timely reporting and timely filings with regulatory agencies.

The category in which an objective falls may vary depending on the circumstances. For instance, controls to prevent theft of assets—such as maintaining a fence around inventory, or having a gatekeeper to verify proper authorization of requests for movement of goods—fall under the operations category. These controls may not be relevant to reporting where inventory losses are detected after a periodic physical inspection and recording in the financial statements. However, if for reporting purposes management relies solely on perpetual inventory records, as may be the case for interim or internal financial reporting, the physical security controls would then also fall within the reporting category. These physical security controls, along with controls over the perpetual inventory records, are needed to achieve reporting objectives. A clear understanding is needed of the entity's business processes, policies and procedures, and the respective impact on each category of objectives.

Basis of Objectives Categories

Some objectives are derived from the regulatory or industry environments in which the entity operates. For example:

- Some entities submit information to environmental agencies.
- Publicly traded companies file information with securities regulators.
- Universities report grant expenditures to government agencies.

These objectives are established largely by law or regulation, and fall into the category of compliance, external reporting, or, in these examples, both.

Conversely, operations and internal reporting objectives are based more on the organization's preferences, judgments, and choices. These objectives vary widely among entities simply because informed and competent people may select different objectives. For example, one organization might choose to be an early adopter of emerging technologies in developing new products, whereas another might be a quick follower, and yet another a late adopter. These choices would reflect the entity's strategies and the competencies, technologies, and controls within its research and development function. Consequently, no one formulation of objectives can be optimal for all entities.

Objectives and Sub-Objectives

Management links specified entity-level objectives to more specific sub-objectives that cascade throughout the organization. Sub-objectives also are established as part of or flowing from the strategy-setting process, and relate to the entity and its subunits and functional activities such as sales, production, engineering, marketing, productivity, employee engagement, innovation, and information technology. Management aligns these sub-objectives with entity-level objectives and coordinates these across the entity.

Where entity-level objectives are consistent with prior practice and performance, the linkage between activities is usually known. Where objectives depart from an entity's past practices, management addresses the linkages or accepts increased risks. For example, an entity-level objective relating to customer satisfaction depends on linked sub-objectives dealing with the introduction of services that use a newer and less proven technology infrastructure. These sub-objectives might need to be substantially changed if past practice used older, proven technologies.

Sub-objectives for operating units and functional activities also need to be specific, measurable or observable, attainable, relevant, and time-bound. In addition, they must be readily understood by the people who are working toward achieving them. Management and other personnel require a mutual understanding of both what is to be accomplished and the means of determining to what extent it is accomplished in order to ensure individual and team accountability.

Entities may specify multiple sub-objectives for each activity, flowing both from the entity-level objectives and from established standards relating to compliance and reporting objectives, as deemed suitable in the circumstances. For example, procurement operations objectives may be to:

- Purchase goods that meet established engineering specifications.
- Purchase goods from companies that meet the entity's environmental, health, and safety specifications as set forth in a code of conduct (e.g., no child labor, good working conditions).
- Negotiate acceptable prices and other terms.

As another example, when specifying suitable external reporting objectives relating to the preparation of external financial statements, management considers accounting standards, financial statement assertions, and qualitative characteristics that are applicable to the entity and its subunits. For example, management may set an entity-level external financial reporting objective as follows: "Our company prepares reliable financial statements reflecting transactions and events in accordance with generally accepted accounting principles."

Management also specifies suitable sub-objectives for divisions, subsidiaries, operating units, and functions with sufficient clarity to support entity-level objectives. For instance, management specifies sub-objectives for sales transactions that apply appropriate accounting standards based on the circumstances and that address relevant financial statement assertions and qualitative characteristics, such as

- All sales transactions that occur are recorded on a timely basis.
- Sales transactions are recorded at correct amounts in the right accounts.
- Sales transactions are accurately and completely summarized in the entity's books and records.
- Presentation and disclosures relating to sales are properly described, sorted, and classified.

Principles of the Internal Control Framework

Role of Principles

Principles are fundamental concepts associated with components. As such, the Framework views the seventeen principles as suitable to all entities. Relevance refers to a determination that each principle has a significant bearing on the presence and functioning of its associated component.

The Framework presumes that principles are relevant. However, there may be a rare industry, operating, or regulatory situation in which management has determined that a principle is not relevant to the associated component. Considerations in applying this judgment may include the entity structure recognizing any legal, regulatory, industry, or contractual requirements for governance of the entity, and the level of use and dependence on technology used by the entity.

If management decides that a principle is not relevant, management must support that determination, including the rationale of how, in the absence of that principle, the associated component could be present and functioning. When a relevant principle is deemed not to be present and functioning, a major deficiency exists in the system of internal control.

In determining whether a component is present and functioning, senior management and the board of directors need to determine to what extent relevant principles are present and functioning. However, a principle being present and functioning does not imply that the organization strives for the highest level of performance in applying that particular principle. Rather, management exercises judgment in balancing the cost and benefit of designing, implementing, and conducting internal control.

Listing of all principles for the integrated framework

Control Environment

The control environment is the set of standards, processes, and structures that provide the basis for carrying out internal control across the organization. The board of directors and senior management establish the tone at the top regarding the importance of internal control and expected standards of conduct.

1. *The organization demonstrates a commitment to integrity and ethical values.*
2. *The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.*
3. *Management establishes, with board oversight, 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 in alignment with objectives.*
5. *The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.*

Risk Assessment

Risk assessment involves a dynamic and iterative process for identifying and analyzing risks to achieving the entity's objectives, forming a basis for determining how risks should be managed. Management considers possible changes in the external environment and within its own business model that may impede its ability to achieve its objectives.

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.*
8. *The organization considers the potential for fraud in assessing risks to the achievement of objectives.*
9. *The organization identifies and assesses changes that could significantly impact the system of internal control.*

Control Activities

Control activities are the actions established by policies and procedures to help ensure that management directives to mitigate risks to the achievement of objectives are carried out. Control activities are performed at all levels of the entity and at various stages within business processes, and over the technology environment.

10. *The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.*
11. *The organization selects and develops general control activities over technology to support the achievement of objectives.*
12. *The organization deploys control activities through policies that establish what is expected and in procedures that put policies into action.*

Information and Communication

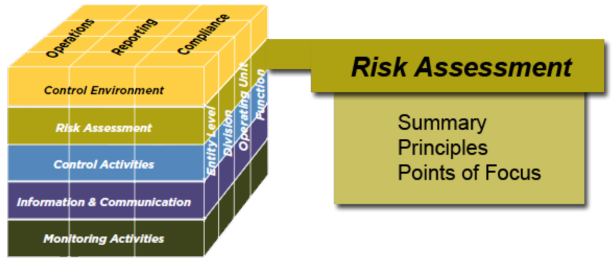
Information is necessary for the entity to carry out internal control responsibilities in support of achievement of its objectives. Communication occurs both internally and externally and provides the organization with the information needed to carry out day-to-day controls. Communication enables personnel to understand internal control responsibilities and their importance to the achievement of objectives.

13. *The organization obtains or generates and uses relevant, quality information to support the functioning of other components of internal control.*
14. *The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of other components of internal control.*
15. *The organization communicates with external parties regarding matters affecting the functioning of other components of internal control.*

Monitoring Activities

Ongoing evaluations, separate evaluations, or some combination of the two are used to ascertain whether each of the five components of internal control, including controls to effect the principles within each component, is present and functioning. Findings are evaluated and deficiencies are communicated in a timely manner, with serious matters reported to senior management and to the board.

16. *The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.*
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 directors, as appropriate.*



Summary

Every entity faces a variety of risks from external and internal sources. Risk is defined as the possibility that an event will occur and adversely affect the achievement of objectives. Risk assessment involves a dynamic and iterative process for identifying and assessing risks to the achievement of objectives. Risks to the achievement of these objectives from across the entity are considered relative to established risk tolerances. Thus, risk assessment forms the basis for determining how risks will be managed. A precondition to risk assessment is the establishment of objectives, linked at different levels of the entity. Management specifies objectives within categories relating to operations, reporting, and compliance with sufficient clarity to be able to identify and analyze risks to those objectives. Management also considers the suitability of the objectives for the entity. Risk assessment also requires management to consider the impact of possible changes in the external environment and within its own business model that may render internal control ineffective.

All entities, regardless of size, structure, nature, or industry, encounter risks at all levels. Risk is defined in the Framework as the possibility that an event will occur and adversely affect the achievement of objectives.

The use of the term "adversely" in this definition does not ignore positive variances relating to an event or series of events. Large positive variances may still create adverse impacts to objectives. For instance, consider a company that forecasts sales of 1,000 units and sets production schedules to achieve this expected demand. Management considers the possibility that actual orders will exceed this forecast. Actual orders of 1,500 units would likely not impact the sales objectives but might adversely impact production costs (through incremental overtime needed to meet increased volumes) or customer satisfaction targets (through increased back orders and wait times). Consequently, selling more units than planned may adversely impact objectives other than the sales objective.

As part of the process of identifying and assessing risks, an organization may also identify opportunities, which are the possibility that an event will occur and positively affect the achievement of objectives. These opportunities are important to capture and to communicate to the objective-setting processes. For instance, in the above example, management would channel new sales opportunities to the objective-setting processes. However, identifying and assessing potential opportunities such as new sales opportunities is not a part of internal control.

Risks affect an entity's ability to succeed, compete within its industry, maintain its financial strength and positive reputation, and maintain the overall quality of its products, services, and people. There is no practical way to reduce risk to zero. Indeed, the decision to be in business incurs risk. Management must determine how much risk is to be prudently accepted, strive to maintain risk within these levels, and understand how much tolerance it has for exceeding its target risk levels.

Risk often increases when objectives differ from past performance and when management implements change. An entity often does not set explicit objectives when it considers its performance to be acceptable. For example, an entity might view its historical service to customers as acceptable and therefore not set specific goals on maintaining current levels of service. However, as part of the risk assessment process, the organization does need to have a common understanding of entity-level objectives relevant to operations, reporting, and compliance and how those cascade into the organization.

Risk Tolerance

Risk tolerance is the acceptable level of variation in performance relative to the achievement of objectives. Operating within risk tolerance provides management with greater confidence that the entity will achieve its objectives. Risk tolerance may be expressed in different ways to suit each category of objectives. For instance, when considering financial reporting, risk tolerance is typically expressed in terms of materiality, whereas for compliance and operations, risk tolerance is often expressed in terms of the acceptable level of variation in performance.

Risk tolerance is normally determined as part of the objective-setting process, and as with setting objectives, setting tolerance levels is a precondition for determining risk responses and related control activities. Management may exercise significant discretion in setting risk tolerance and managing risks when there are no external requirements. However, when there are external requirements, such as those relating to external reporting and compliance objectives, management considers risk tolerance within the context of established laws, rules, regulations, and external standards.

As well, senior management considers the relative importance of the competing objectives and differing priorities for pursuing these objectives. For instance, a chief operating officer may view operations objectives as requiring a higher level of precision than materiality considerations in reporting objectives, and vice versa for the chief financial officer. However, it would be problematic for public companies to overemphasize operational objectives to an extent that adversely impacts the reliability of financial reporting. These views are considered as part of the strategic-planning and objective-setting process with tolerances set accordingly. This kind of decision may also impact the level of resources allocated to pursuing the achievement of those respective objectives.

Principles relating to the Risk Assessment component

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.*

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

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

Specifies Suitable Objectives

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

Points of Focus

The following points of focus may assist management in determining whether this principle is present and functioning:

A precondition to risk assessment is the establishment of objectives, linked at various levels of the entity. These objectives align with and support the entity in the pursuit of its strategic direction. While setting strategies and objectives is not part of the internal control process, objectives form the basis on which risk assessment approaches are implemented and performed and subsequent control activities are established. As part of internal control, management specifies objectives and groups them within broad categories at all levels of the entity, relating to operations, reporting, and compliance. The grouping of objectives within these categories allows for the risks to the achievement of those objectives to be identified and assessed.

In considering the suitability of objectives, management may consider such matters as:

- Alignment between established objectives and strategic priorities
- Articulation of risk tolerances for objectives
- Alignment between established objectives and established laws, rules, regulations, and standards applicable to the entity
- Articulation of objectives using terms that are specific, measurable or observable, attainable, relevant, and time-bound
- Cascading of objectives across the entity and it subunits
- Alignment of objectives to other circumstances that require specific focus by the entity
- Approval objectives within the objective-setting process

Where objectives within these categories are unclear, where it is unclear how these objectives support the strategic direction, or where there are concerns that the objectives are not suitable based on the facts, circumstances, and established laws, rules, regulations, and standards applicable to the entity, management communicates this concern for input to the strategy-setting and objective-setting process.

Operations Objectives

<u>Points of Focus</u>
The following points of focus may assist management in determining whether this principle is present and functioning:

- **Reflects Management's Choices**—Operations objectives reflect management's choices about structure, industry considerations, and performance of the entity.
- **Considers Tolerances for Risk**—Management considers the acceptable levels of variation relative to the achievement of operations objectives.
- **Includes Operations and Financial Performance Goals**—The organization reflects the desired level of operations and financial performance for the entity within operations objectives.
- **Forms a Basis for Committing of Resources**—Management uses operations objectives as a basis for allocating resources needed to attain desired operations and financial performance.

Reporting Objectives

Reporting objectives pertain to the preparation of reports that encompass reliability, timeliness, transparency, or other terms as set forth by regulators, standard-setting bodies, or by the entity's policies. This category includes external financial reporting, external non-financial reporting, internal financial reporting, and internal non-financial reporting. External reporting objectives are driven primarily by laws, rules, regulations, and standards established by governments, regulators, standard-setting bodies, and accounting bodies. Internal reporting objectives are driven by the entity's strategic directions, and by reporting requirements and expectations established by management and the board of directors.

External Financial Reporting

<u>Points of Focus</u>
The following points of focus may assist management in determining whether this principle is present and functioning as it relates to external financial reporting objectives:

- **Complies with Applicable Accounting Standards**—Financial reporting objectives are consistent with accounting principles suitable and available for that entity. The accounting principles selected are appropriate in the circumstances.

- **Considers Materiality**—Management considers materiality in financial statement presentation.
- **Reflects Entity Activities**—External reporting reflects the underlying transactions and events to show qualitative characteristics and assertions.

External Non-Financial Reporting

Points of Focus
The following points of focus may assist management in determining whether this principle is present and functioning as it relates to external non-financial reporting objectives:

- **Complies with Externally Established Standards and Frameworks**—Management establishes objectives consistent with laws and regulations, or standards and frameworks of recognized external organizations.
- **Considers the Required Level of Precision**—Management reflects the required level of precision and accuracy suitable for user needs and as based on criteria established by third parties in non-financial reporting.
- **Reflects Entity Activities**—External reporting reflects the underlying transactions and events within a range of acceptable limits.

Internal Reporting Objectives

Points of Focus
The following points of focus may assist management in determining whether this principle is present and functioning as it relates to internal reporting objectives:

- **Reflects Management's Choices**—Internal reporting provides management with accurate and complete information regarding management's choices and information needed in managing the entity.
- **Considers the Required Level of Precision**—Management reflects the required level of precision and accuracy suitable for user needs in non-financial reporting objectives and materiality within financial reporting objectives.
- **Reflects Entity Activities**—Internal reporting reflects the underlying transactions and events within a range of acceptable limits.

Compliance Objectives

Points of Focus
The following points of focus may assist management in determining whether this principle is present and functioning as it relates to compliance objectives:

- **Reflects External Laws and Regulations**—Laws and regulations establish minimum standards of conduct which the entity integrates into compliance objectives.
- **Considers Tolerances for Risk**—Management considers the acceptable levels of variation relative to the achievement of compliance objectives.

Identifies and Analyzes Risk

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.

Points of Focus
The following points of focus may assist management in determining whether this principle is present and functioning:

- **Includes Entity, Subsidiary, Division, Operating Unit, and Functional Levels**—The organization identifies and assesses risks at the entity, subsidiary, division, operating unit, and functional levels relevant to the achievement of objectives.
- **Analyzes Internal and External Factors**—Risk identification considers both internal and external factors and their impact on the achievement of objectives.
- **Involves Appropriate Levels of Management**—The organization puts into place effective risk assessment mechanisms that involve appropriate levels of management.
- **Estimates Significance of Risks Identified**—Identified risks are analyzed through a process that includes estimating the potential significance of the risk.
- **Determines How to Respond to Risks**—Risk assessment includes considering how the risk should be managed and whether to accept, avoid, reduce, or share the risk.

Assesses Fraud Risk

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

Points of Focus

The following points of focus may assist management in determining whether this principle is present and functioning:

- **Considers Various Types of Fraud**—The assessment of fraud considers fraudulent reporting, possible loss of assets, and corruption resulting from the various ways that fraud and misconduct can occur.
- **Assesses Incentive and Pressures**—The assessment of fraud risk considers incentives and pressures.
- **Assesses Opportunities**—The assessment of fraud risk considers opportunities for unauthorized acquisition, use, or disposal of assets, altering of the entity's reporting records, or committing other inappropriate acts.
- **Assesses Attitudes and Rationalizations**—The assessment of fraud risk considers how management and other personnel might engage in or justify inappropriate actions.

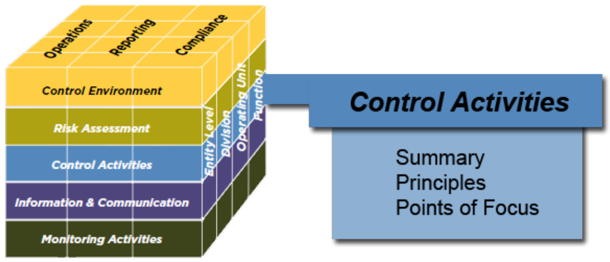
Identifies and Analyzes Significant Change

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

Points of Focus

The following points of focus may assist management in determining whether this principle is present and functioning:

- **Assesses Changes in the External Environment**—The risk identification process considers changes to the regulatory, economic, and physical environment in which the entity operates.
- **Assesses Changes in the Business Model**—The organization considers the potential impacts of new business lines, dramatically altered compositions of existing business lines, acquired or divested business operations on the system of internal control, rapid growth, changing reliance on foreign geographies, and new technologies.
- **Assesses Changes in Leadership**—The organization considers changes in management and respective attitudes and philosophies on the system of internal control.



Summary

Control activities are the actions established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out. Control activities are performed at all levels of the entity, at various stages within business processes, and over the technology environment. They may be preventive or detective in nature and may encompass a range of manual and automated activities such as authorizations and approvals, verifications, reconciliations, and business performance reviews. Segregation of duties is typically built into the selection and development of control activities. Where segregation of duties is not practical, management selects and develops alternative control activities.

Control activities serve as mechanisms for managing the achievement of an entity's objectives and are very much a part of the processes by which an entity strives to achieve those objectives. They do not exist simply for their own sake or because having them is the right or proper thing to do.

Control activities can support one or more of the entity's operations, reporting, and compliance objectives. For example, an online retailer's controls over the security of its information technology affect the processing of accurate and valid transactions with consumers, the protection of consumers' confidential credit card information, and the availability and security of its website. In this case, control activities are necessary to support the reporting, compliance, and operations objectives.

Principles relating to the Control Activities component

10. *The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.*

11. *The organization selects and develops general control activities over technology to support the achievement of objectives.*

12. *The organization deploys control activities through policies that establish what is expected and in procedures that put policies into action.*

Selects and Develops Control Activities

Principle 10: The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

Points of Focus

The following points of focus may assist management in determining whether this principle is present and functioning:

- **Integrates with Risk Assessment**—Control activities help ensure that risk responses that address and mitigate risks are carried out.
- **Considers Entity-Specific Factors**—Management considers how the environment, complexity, nature, and scope of its operations, as well as the specific characteristics of its organization, affect the selection and development of control activities.

- **Determines Relevant Business Processes**—Management determines which relevant business processes require control activities.
- **Evaluates a Mix of Control Activity Types**—Control activities include a range and variety of controls and may include a balance of approaches to mitigate risks, considering both manual and automated controls, and preventive and detective controls.

Selects and Develops General Controls over Technology

Principle 11: The organization selects and develops general control activities over technology to support the achievement of objectives.

Points of Focus
The following points of focus may assist management in determining whether this principle is present and functioning:

- **Determines Dependency between the Use of Technology in Business Processes and Technology General Controls**—Management understands and determines the dependency and linkage between business processes, automated control activities, and technology general controls.
- **Establishes Relevant Technology Infrastructure Control Activities**—Management selects and develops control activities over the technology infrastructure, which are designed and implemented to help ensure the completeness, accuracy, and availability of technology processing.
- **Establishes Relevant Security Management Process Control Activities**— Management selects and develops control activities that are designed and implemented to restrict technology access rights to authorized users commensurate with their job responsibilities and to protect the entity's assets from external threats.
- **Establishes Relevant Technology Acquisition, Development, and Maintenance Process Control Activities**—Management selects and develops control activities over the acquisition, development, and maintenance of technology and its infrastructure to achieve management's objectives.

Deploys through Policies and Procedures

Principle 12: The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.

Points of Focus
The following points of focus may assist management in determining whether this principle is present and functioning:

- **Establishes Policies and Procedures to Support Deployment of Management's Directives**—Management establishes control activities that are built into business processes and employees' day-to-day activities through policies establishing what is expected and relevant procedures specifying actions.
- **Establishes Responsibility and Accountability for Executing Policies and Procedures**—Management establishes responsibility and accountability for control activities with management (or other designated personnel) of the business unit or function in which the relevant risks reside.
- **Performs in a Timely Manner**—Responsible personnel perform control activities in a timely manner as defined by the policies and procedures.
- **Takes Corrective Action**—Responsible personnel investigate and act on matters identified as a result of executing control activities.
- **Performs Using Competent Personnel**—Competent personnel with sufficient authority perform control activities with diligence and continuing focus.
- **Reassesses Policies and Procedures**—Management periodically reviews control activities to determine their continued relevance, and refreshes them when necessary.

James Houser University
A Case Study in Internal Control

Overview and Background:

James Houser University (JHU) was founded in Los Angeles, California, USA in 1965 in response to the riots in the Watts area of Los Angeles. On the heels of the federal legislation concerning civil rights, communities began changes to implement the new laws. One of the underlying causes of the unrest and riots in the Watts community was directly related to poor, and often total lack of health services to the underserved populous in the Los Angeles area. JHU was created to bridge that gap to help provide full health services to all community members, regardless of race or national origin.

A new complex was funded by state and federal funds to build a full service medical complex which included outpatient facilities, a hospital, and an education and training facility. The vision was to locate the facility in the heart of the community and draw community members to serve as professionals in the new health care and hospital. The education and training center would generate doctors, nurses, technicians and related hospital staff to serve in the community medical complex. This plan provided the needed health care services with long run impact on the jobless and economic conditions of the communities. In short, the community would be served by itself, payroll going to members of the community creating professional jobs and greatly impacting the jobless circumstance of the community.

The State of California pioneered a grant program through California State University (CSU) to fund a new university to educate and train medical professionals from the community to accomplish the vision and provide quality medical services to the community. California State deliberated and believed it more appropriate to use the grant funds to create a new facility and organization in the local community independent of CSU. The university would remain as the principal grantee and would control the funds and quality of education, but would award the funds as a sub award to a secondary grantee, the new organization in the community. This approach would make the education easily accessible and affordable by community members wishing to become medical providers, rather than using CSU's established campus over forty miles from the community. The plan was approved by the state legislature.

In 1965, one year after the legislation and funds made available by the state and federal authorities, James Houser University was founded in the community to serve as the source of the education and training as legislated by the state. JHU was appropriated state purchased and donated land adjoining a new medical facility which was under construction, built with state funds and private contributions. By the end of 1965, funds were made available from a variety of sources to build the new campus and equip it as needed. It opened its doors in early 1966. Its stated mission was: *to create and provide quality health and medical services to the underserved community while positively impacting the local economy and employment opportunities of the residents.*

The hospital and medical complex was named after the famed civil rights leader Dr. Martin Luther King (MLK). The university was named in honor Dr. James J. Houser (deceased), an African American physician who was internationally known for his work in kidney research and related disease treatment. The two facilities operated independently from each other, both created as non-profit corporations. The MLK hospital and medical center over the last decades has been staffed primarily with graduates from the JHU programs. Specialists and independent practitioners have migrated to the area to fill needs not met by the flow of graduates from JHU.

Both facilities have survived and grown over the past forty five years with creative approaches to funding including state and federal appropriations, contributions from foundations, insurance coverage and payments, local and community grants and programs. Charges for care are administered based on the economic situation of the recipient through a variety of programs. Those who can afford the care are charged at cost since the medical complex is a non-profit corporation.

Recent History of the University:

Medical and Technical Programs

Over the past two decades, from approximately 1997 to 2018, the university has dramatically expanded its operations. New curriculums and degree offerings in technical programs related to the advancements in digital and automated tools and services have surged to meet the demands in the MLK hospital as well as feeding graduates to other facilities in the Los Angeles area. A majority of the growth has been funded by student grants from state and national organizations. As well, student loan programs are available with ease of access due to the continued classification of the JHU residing in an underserved community. The student fees and tuition amount to about $5 million USD annually.

The Medical College

In the past two years, the medical college has grown from twenty medical students to an average of twenty seven students. Graduates rate very high on national exams and rating systems. The quality of the faculty at JHU has increased dramatically over the past two decades due primarily to the expanded emphasis on research and research funding. Professors are drawn to the university because it supports their efforts in obtaining grants as supplements to their teaching salaries. Grant income as a researcher often exceeds the professor's salary for teaching. As well, the collaborative interaction with a strong research organization enhances the quality and outcome of the research endeavors. The grant from CSU to fund the medical school and its students is currently at $10 million USD and is expected to be cut by 20% by the California legislature due to excessive state budget deficits. Current medical students incur very little tuition and are almost fully supported by the grant fund from CSU. As a result, entry requirements and criteria can be set very high. New students may have to locate additional funding from loans and personal grants to cover loss of funding from the state budget.

The Research Division

In 2010, due to the amount and rapid growth in the research area, a new division of the university was created and a new Vice President of Research position was developed. Carl Maddix, PhD, MD, was appointed to the position when it was created and has retained the responsibilities since 2010. Dr. Maddix is a superb researcher and is personally responsible for strong growth in the research area since assuming the role of VP in 2010. The total amount of externally funded research has grown from $14 million USD in 2010 to a level of $60 million USD in 2018. Dr. Maddix is the principal investigator on over $10 million USD of the total grant budget of $40 million, constituting roughly 25% of the grant funds flow.

The research funding has become the majority of funds budget in 2018. Total budget for 2018 was approximately $80 million USD, with external research funding comprising $60 million USD of that amount, roughly three fourths of the university budget. To meet this administrative and executive load for grant oversight, Dr. Maddix created a position entitled Associate Vice President of Research and employed a colleague of his to fill the position. Dr. Maddix used a combination of grant direct funds and indirect funds to pay for the new position. Ray Blunt, PhD was employed on a one half time (50%) full time equivalent to staff the position. Dr. Blunt is a colleague and co-principal investigator with Dr. Maddix on a substantial federal grant program.

University Administration

The university has experienced a series of turnovers in the President's position over the past decade. Dr. Martin Lew was President from 2003-16 and retired after twenty years of service to the university as a professor, researcher and executive. Jandy Lisson, MD, PhD took over as President and CEO in 2016 and has been operating in that position since. Dr. Lisson is a British citizen and has extended visa rights in the United States. She has served the university since 2013 as a professor and Assistant Dean of the Medical Programs, assuming the President's slot in 2016. She had no prior executive or administrative experience, her career has been spent as a teaching professor and dean.

During the past two years, Dr. Lisson has made significant changes to the university administration, its composition and systems. She undertook an initiative to replace the accounting and financial reporting system with a cost of just under $3 million USD. The conversion took over a year with large amounts of fees paid to external contractors, but without the full success of the system changeover. In reaction, Dr.

Lisson replaced the Vice President of Finance and his immediate staff with outsourced consultants from the firm of Dalmouth and Associates, placing blame on the VP for not being able to complete the transition.

In an attempt to review the human resource function and processes, Dr. Lisson engaged DynaResources, a firm run by her friend and associate. DynaResources accomplished a thirty day study and presented the results to Dr. Lisson that indicated the human resource department to be substantially substandard in most, if not in all areas of personnel and human resource functioning. In one swoop, Dr. Lisson engaged DynaResources to assume the total functioning of the human resources division as outsourced consultants. On September 1, 2016, Dr. Lisson and the DynaResources team walked into the JHU Human Resources Division and terminated the current staff consisting of: a Human Resources Director; two Human Resources Managers (Employment and Benefits); three HR Administrators; an Administrative Assistant. None of the employees had any idea that their positions were in jeopardy or subject to immediate termination. Their dismissal came as a total shock to them and everyone in the university.

The other administrative directors became very concerned about, as they called them “the rash actions of Dr. Lisson,” and began to assert their objections to the outsourcing of two of the university’s most critical administrative and control functions. When the Director of Information Technology commented in a management meeting to Dr. Lisson that, “you don’t have a clue about what you are doing…the new accounting system does not work, HR is now not functioning…soon we will experience severe reporting and staffing problems.” Within hours after that meeting, Dr. Lisson had terminated the IT Director and placed IT under the management of the Assistant Dean of Medical Programs, a former subordinate of hers.

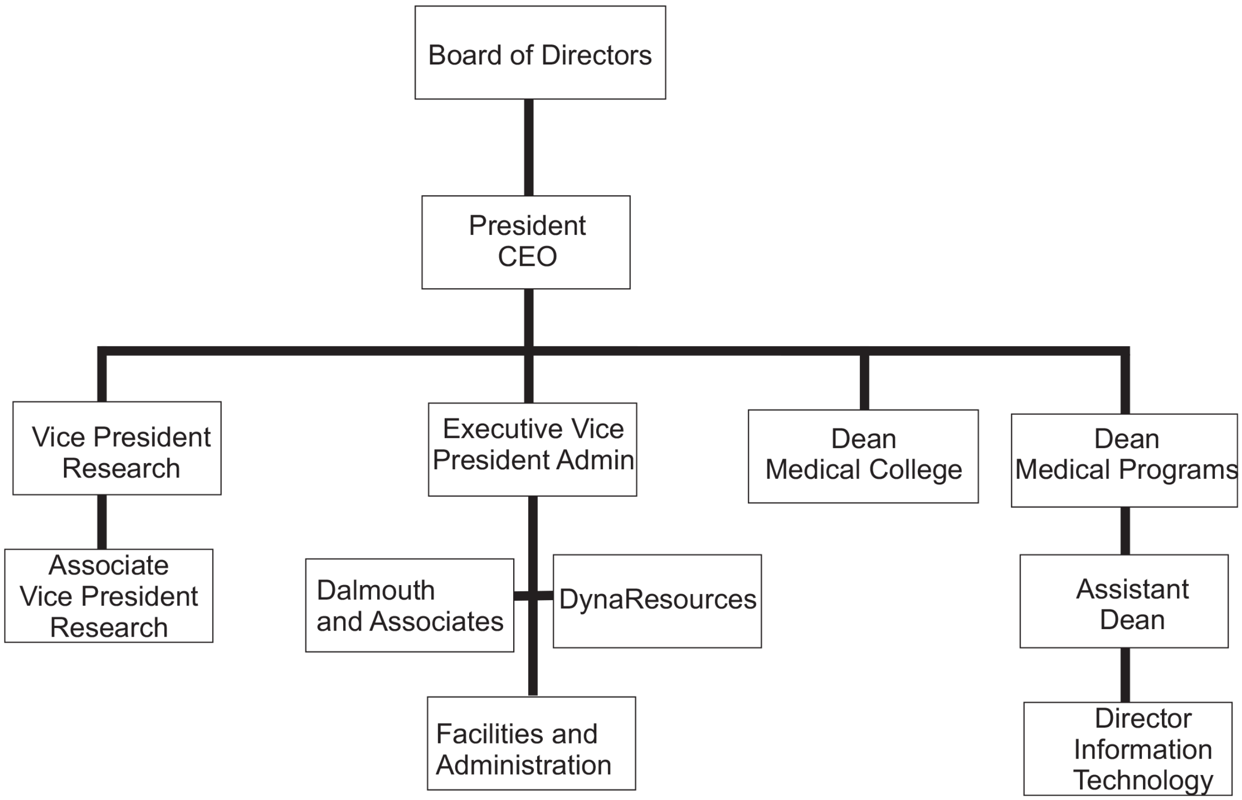
Feeling overwhelmed by the changes she had made, Dr. Lisson created a new position entitled Executive Vice President of Administration and placed all functions under this position. There was no search or open application process for the position. She recruited Nancy Delgado, an administrator from the county health services that Dr. Lisson had befriended in her position as Assistant Dean. Ms. Delgado’s experience had been in county funds administration in a series of small county funded health facilities. She had no executive level or advanced administrative level experience. She was appointed on November 1, 2016 to run all of JHU’s administrative and executive functions and to oversee the $80 million USD university budget.

Board of Directors
Over the life of the university, the composition and makeup of the board has experienced a swing from local community leaders acting as champions for the local residents to members who are appointed due to political or social service contributions from their respective organizations. The Chairman of the Board is Silas Mertins, Esq. a partner in a large Los Angeles law firm. His position on the board serves as his community service requirement in the firm’s partner performance measurement criteria. The firm allows him time to participate during normal working hours and allows for travel when necessary. Mr. Mertins is a very skilled litigator and successful legal practitioner. Other than this position with the university, Mr. Mertins has no other executive or advanced level of administrative experience.

Other board members consist of: the Public Relations Director of a statewide bank; an Associate Director of a small health clinic in greater Los Angeles; a partner in a community real estate firm; a retired professor from the university; a small business executive from retail; a member of the California legislature from the area’s district.

For the last five years, the board has been very agreeable with the recommendations and proposals of the President and CEO. Dr. Lew was very deliberate in his proceedings and the outcomes of his proposals were generally very good to excellent. The board took the same ‘hands off’ approach with Dr. Lisson, providing only cursory review of her proposals prior to acceptance. All of Dr. Lisson’s actions relative to the administrative changes were presented to and approved by the board of directors.

James Houser University
Organzational Chart



Michael L. Piazza
Instructor and Consultant

Michael is the Principal Associate and lead consultant of Professional Development Associates (PDA) and is the managing editor and publisher of the PDA websites. His education includes a BBA in Accountancy, a Masters of Accountancy Degree, and an MBA Degree. The majority of Michael's career has been devoted to professional and organizational development with a focus in instruction and consulting in internal control, governance and related organizational applications. Michael has served the Institute of Internal Auditors (IIA) in various capacities for nearly four decades: Staff Instructor 1980-85; Consultant 1986-1992 and 2003-2008; Committee of Research and Education Advisors Member 2011-2013; IIA Central Mississippi Chapter Vice President then President 2004-2006.

Michael began PDA in 1996 providing performance management and internal control consulting to over 30 state agencies and regional companies. He resumed his international travel in 2003 as a consulting instructor for The Institute of Internal Auditors serving private and public sector organizations. As an instructor, Michael's specialties are: the COSO based internal control framework and applications; operational auditing; internal audit processes and supervision.

In response to the Committee of Sponsoring Organizations (COSO) release of the updated Internal Control Integrated Framework of May 2013, Michael created and published a web site dedicated to the new framework: controlsframework.com. The site is a comprehensive resource offering detailed information of the framework, its components, concepts and principles and contains an array of course offerings on the COSO 2013 framework.

Michael provided organizational development and control consulting to Jackson State University (Jackson, MS), Clark Atlanta University (Atlanta, GA) and Charles R. Drew University of Medicine and Science (Los Angeles, CA), working with Principal Investigators and Administrators to enhance and improve compliance controls and business processes, including serving as the chief administrator pioneering the creation and development of the Research Centers in Minority Institutions Translational Research Network (RTRN.net).

As an IIA staff member, Michael served The Institute of Internal Auditors throughout the 1980's in various roles as a Seminar Instructor, Conference Presenter and Program Manager. His manager roles included Manager of College and University Relations, Manager of Continuing Professional Development, Manager of Media Assisted Programs.

After his tenure as staff member and consultant to The IIA, Michael returned to his home state and spent the 1990's as an executive and then as a consultant to state government of Mississippi. He served in various executive capacities including State Policy Director and Director of Compensation for the Mississippi State Personnel Department, and Deputy Director for the Mississippi Arts Commission. He left staff work creating PDA and performed as a consultant to 30+ agencies in performance management and control.

Michael created *The Seventh Code* as a case study when he was the business process consultant on a major database development that combined the payroll and personnel systems of over 120 state agencies. Over time, as the case became popular with his colleagues, he developed it into a fictional suspense novel of 14 chapters and serves as the first novel in a three novel series entitled The CAIN System Trilogy, followed by *King of Rules* and *The Omega Club* (to be published Spring, 2019). The *Seventh Code* has been read by over 2,000 auditors who have really enjoyed the story and its turns. *The Seventh Code* and *King of Rules* are both currently available on Amazon in either Kindle or paperback edition.