RISK BASED INTERNAL AUDIT

Presented by

Humphrey Okorie

(B. Tech, MBA, CIA, CRMA, CISA, CISSP)

Independent Consultant & CEO, IIA Nigeria

Organised by Association of Chief Audit Executives of Banks In Nigeria in conjunction IIA Nigeria

July 14-15 2017

CONTENTS

Part One: Internal Auditing and Risk Based Internal Auditing

- Definition and Role of Internal Auditing
- International Professional Practices Framework for the Professional Practice of Internal Auditing (IPPF)
- Definition and Essence of Risk Based Internal Auditing

Part Two: Risk Management and Enterprise Risk Management

- Definition of Risk and Enterprise Risk Management
- Types of risks and basic risk management concepts
- Performance Standard 2120: Risk Management

CONTENTS

Part Three: Risk and Control Frameworks

- Performance Standard 2130-Control
- COSO Control and ERM frameworks
- Roles and Responsibilities in Internal Control

Part Four: Enterprise wide risk assessment and Audit plan development

- Assurance Performance Standard 2130.A1
- Performing an Enterprise wide risk assessment
- Developing an Internal Audit plan

CONTENTS

Part Five: Risk Based Audit Engagement

- Performing a risk based audit engagement
- Approaches for managing risks and evaluating controls
- Reporting risk based audit engagements

Part Six: Questions & Wrap up

- Conclusion
- Questions

PART ONE: INTERNAL AUDITING AND RISK BASED INTERNAL AUDITING

- Definition and Role of Internal Auditing
- International Professional Practices Framework for the Professional Practice of Internal Auditing (IPPF)
- Definition and Essence of Risk Based Internal Auditing

Definition and Role of Internal Auditing

Definition:

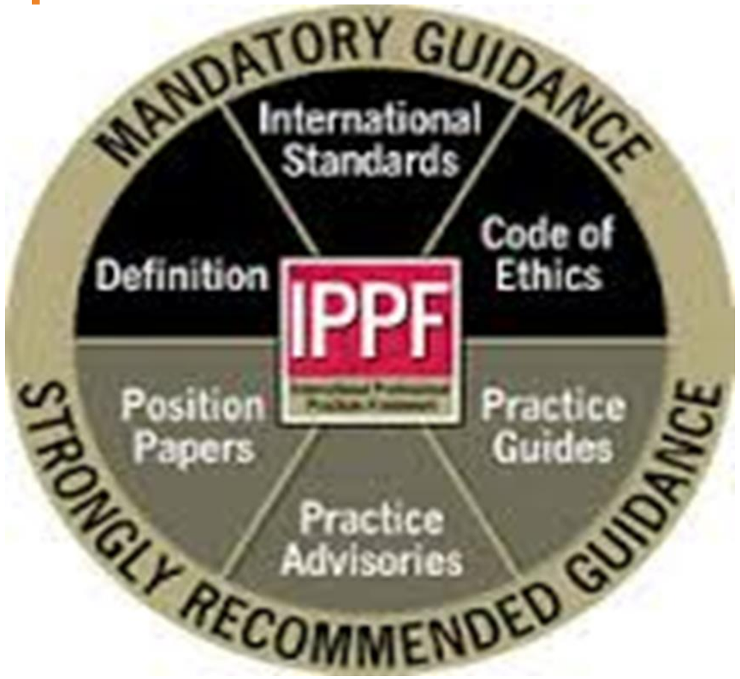
- Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

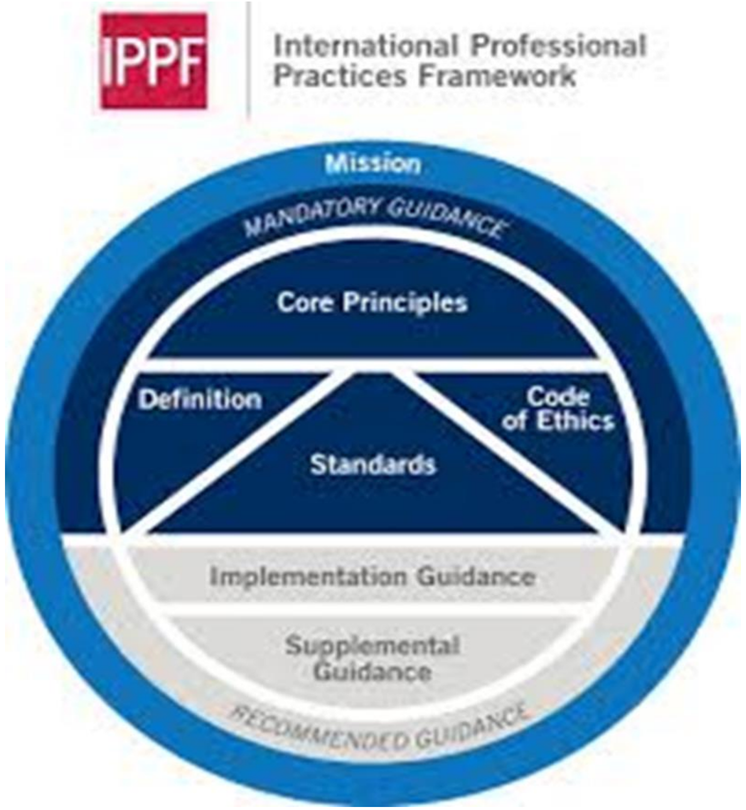
Internal Auditing Standard 2100: Nature of Work

- The internal audit activity must evaluate and contribute to the improvement of the organization's governance, risk management, and control processes using a systematic, disciplined, and risk based approach. Internal audit credibility and value are enhanced when auditors are proactive and their evaluations offer new insights and consider future impact.

International Professional Practices Framework for the Professional Practice of Internal Auditing (IPPF)

Previous IPPF



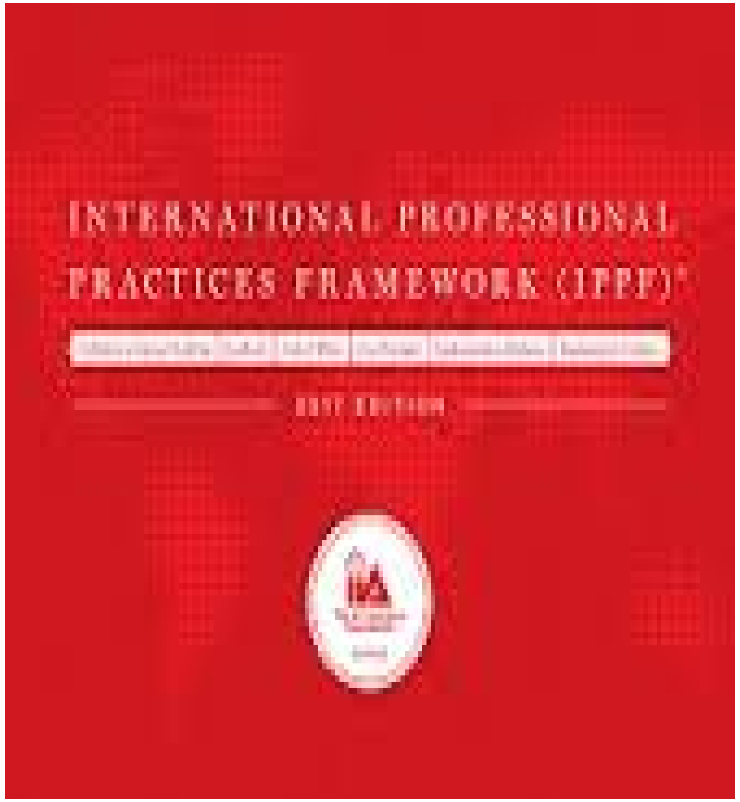


Revised 2017 IPPF

International Professional Practices Framework for the Professional Practice of Internal Auditing (IPPF)

2013 IPPF

Revised 2017 IPPF



's

on

es to

ins from

Definition and Essence of Risk Based Internal Auditing

Definition of Risk Based Internal Audit (RBIA)

- IIA defines *risk based internal auditing* (RBIA) as a methodology that links *internal auditing* to an organisation's overall *risk* management framework. RBIA allows *internal audit* to provide assurance to the board that *risk* management processes are managing risks effectively, in relation to the *risk* appetite.

According to IIA UK & Ireland, RBIA enables internal audit to provide the board with assurance that it needs on three areas:

- Risk management processes, both their design and how well they are working
- Management of those risks classified as 'key', including the effectiveness of the controls and other responses to them
- Complete, accurate and appropriate reporting and classification of risks

RBIA audits the management of key risks, focuses on the areas of the highest risk to the organisation and begins from the business objectives rather than controls

PART TWO: RISK MANAGEMENT AND ENTERPRISE RISK MANAGEMENT

- Definition of Risk and Enterprise Risk Management
- Types of Risks and Basic risk management concepts
- Performance Standard 2120: Risk Management

Definition of Risk Management and Enterprise Risk Management

Risk

- The possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood.

ERM

- A process, affected by an entity's board of directors, management, and other personnel, applied in a strategy setting across the organization. The process is designed to identify potential events that may affect the entity, manage risks to be within its risk appetite, and provide reasonable assurance regarding the achievement of objectives. — COSO ERM

Types of risk and basic risk management concepts

Inherent risk

- Underlying risk before any controls are applied to mitigate the risk

Residual risk

- Remaining after management takes action to reduce the impact and likelihood of an adverse event, including control activities in responding to a risk

Risk Appetite

- Amount and type of *risk* that an organisation is willing to take in order to meet their strategic objectives-Theirm

Risk register or log

Tool for documenting risks, related activities and actions for managing the risks

Categories of risks

- Strategic, Operational , Financial, Compliance, Reputational, Information Technology etc.

Performance Standard 2120: Risk Management

Standard 2120 – Risk Management

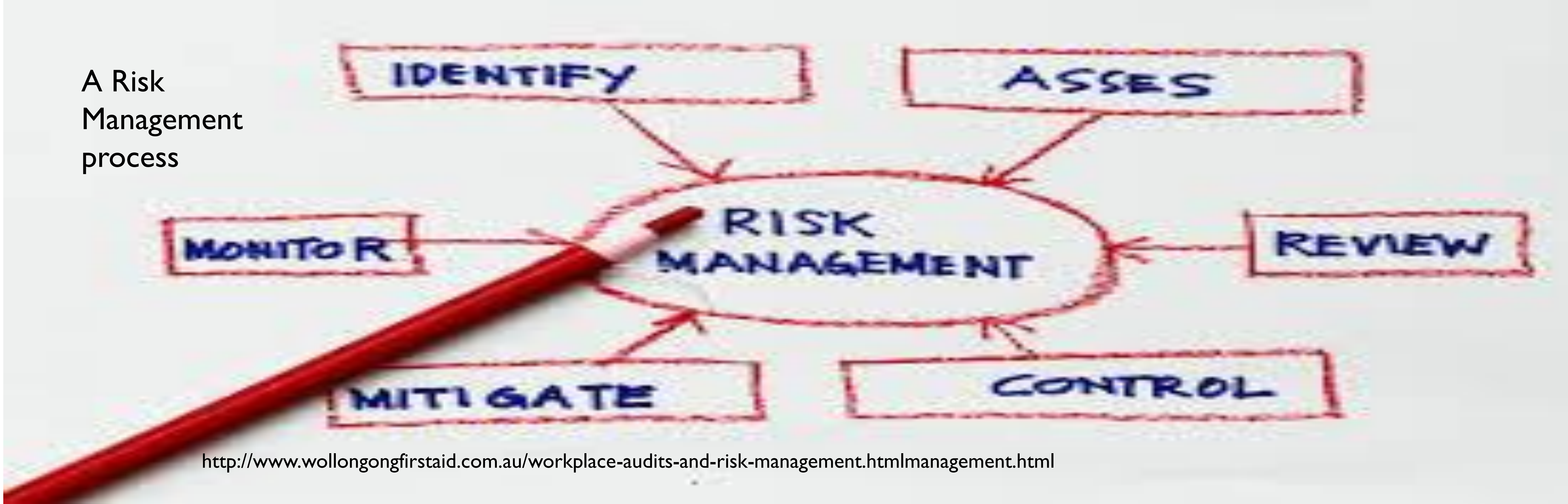
- The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.

Interpretation:

- Determining whether risk management processes are effective is a judgment resulting from the internal auditor's assessment that:
  - Organizational objectives support and align with the organization's mission.
  - Significant risks are identified and assessed.
  - Appropriate risk responses are selected that align risks with the organization's risk appetite.
  - Relevant risk information is captured and communicated in a timely manner across the organization, enabling staff, management, and the board to carry out their responsibilities.

Performance Standard 2120: Risk Management

- The internal audit activity may gather the information to support this assessment during multiple engagements. The results of these engagements, when viewed together, provide an understanding of the organization's risk management processes and their effectiveness.
- Risk management processes are monitored through ongoing management activities, separate evaluations, or both



A Risk Management process

http://www.wollongongfirstaid.com.au/workplace-audits-and-risk-management.htmlmanagement.html

PART THREE: RISK AND CONTROL FRAMEWORKS

- Performance Standard 2130-Control
- COSO Control and ERM frameworks
- Roles and Responsibilities in Internal ControL

Internal Control and Performance Standard 2130-Control

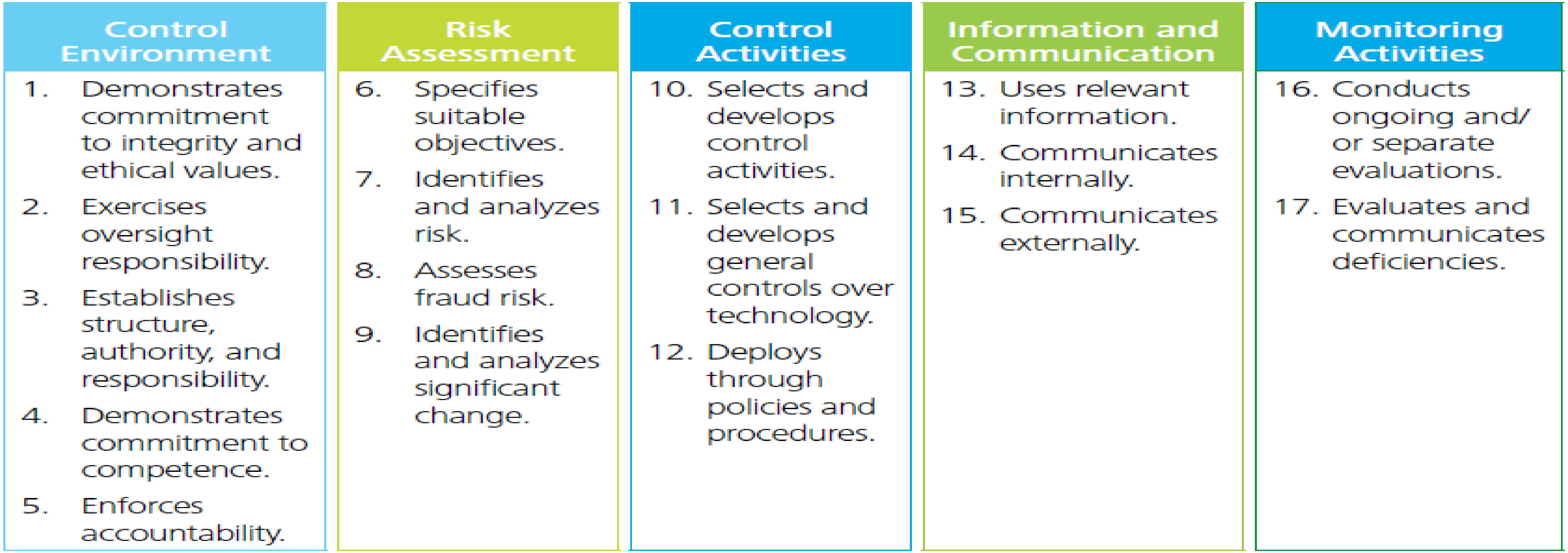
Definition of Internal Control

- Internal control is a process affected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:
  - Effectiveness and efficiency of operations
  - Reliability of reporting
  - Compliance with applicable laws and regulations

Standard 2130 – Control

- The internal audit activity must assist the organization in maintaining effective controls by evaluating their effectiveness and efficiency and by promoting continuous improvement.

COSO Control and ERM frameworks

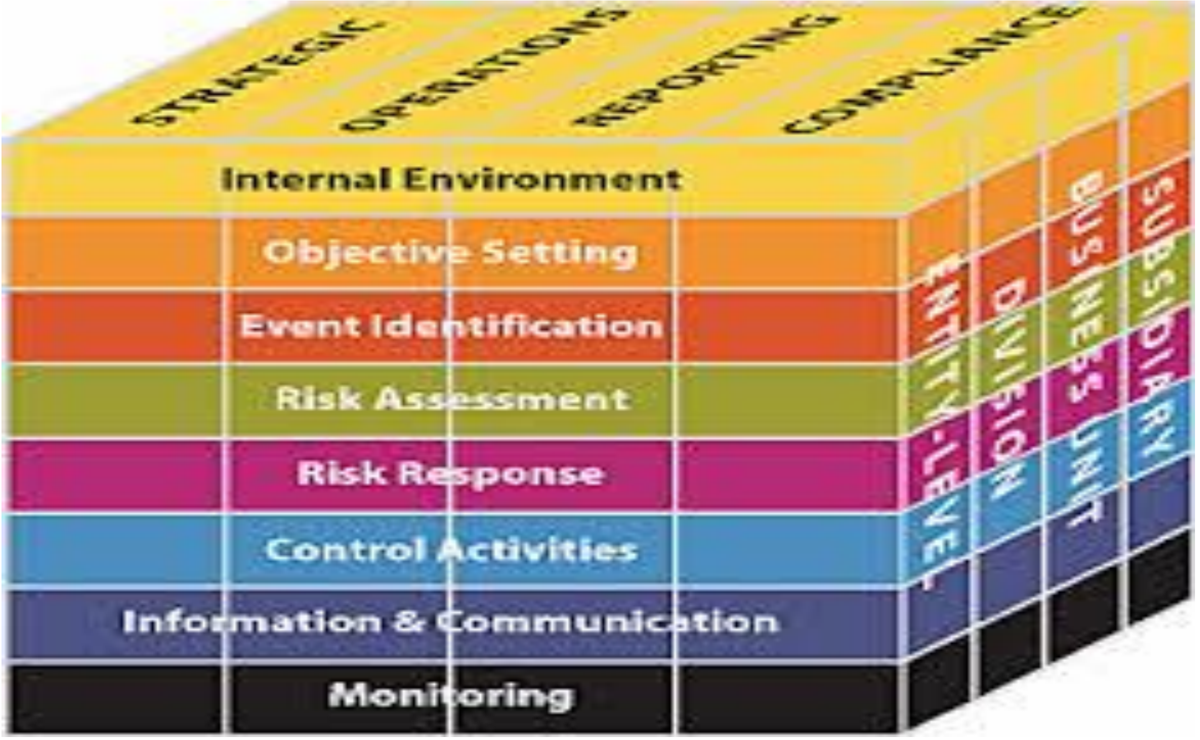


Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring Activities
1. Demonstrates commitment to integrity and ethical values. 2. Exercises oversight responsibility. 3. Establishes structure, authority, and responsibility. 4. Demonstrates commitment to competence.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

COSO Control framework

Deloitte.(2013)

COSO Control and ERM frameworks



COSO Integrated ERM framework

Roles and Responsibilities in Internal ControL

Management owns controls.

- Management can empower others and see this as a partnership.
- Management cannot say they did not know.
- All personnel have control responsibility for their area.

The board of directors provide oversight and guidance.

Internal auditing evaluates effectiveness.

PART FOUR: ENTERPRISE WIDE RISK ASSESSMENT AND AUDIT PLAN DEVELOPMENT

- Assurance Performance Standard 2130.A1
- Performing an Enterprise wide risk assessment
- Developing an Internal Audit plan

Assurance Performance Standard 2130.A1

Standard 2130.A1

The internal audit activity must evaluate the adequacy and effectiveness of controls in responding to risks within the organization's governance, operations, and information systems regarding the:

- Achievement of the organization's strategic objectives.
- Reliability and integrity of financial and operational information.
- Effectiveness and efficiency of operations and programs.
- Safeguarding of assets.
- Compliance with laws, regulations, policies, procedures, and contracts.

Performing an Enterprise wide risk assessment

- Inventory the business processes, activities, or organizations that account for all organizational risks

Use

- focus groups to assist in the identification of risks;
- interviews of key leadership and the board;
- surveys;
- reviews of previous audit findings, external audits conducted in the organization, and identifying what is occurring within the industry and the local market, etc.

Performing an Enterprise wide risk assessment

- After risks have been identified, use prioritization process to identify the
  - likelihood of the risk occurring,
  - ability of management to mitigate risk (i.e. are there controls in place for risk, regardless of the likelihood of those risks of occurring?),
  - impact of risk on the organization.
- Risk prioritization should be an ongoing process and should include periodic reviews during the year to ensure that previous prioritization methods, when applied in real time, are still applicable for the risk
- Senior leadership should participate in, and agree with, the determination of the high-risk priorities for the audit and monitoring plan
- Weight the risk factors, assign relative risk score and gain consensus from the audit committee

Developing an Internal Audit plan

- Inventory the business processes or activities.
- Establish risk factors that apply to all processes or activities.
- Risk rank the auditable universe.
- Assign workload estimates to each unit.
- Assign any coverage rules.
- Develop full coverage plan.
- Consider resources.
- Identify gaps.
- Commit to constrained resources plan.
- Gain consensus from audit committee and management

IIA (2016)

Developing an Internal Audit plan

Considerations

- Review of other business areas in the organization which may be conducting an audit or monitoring activity in this area: –
- If possible leverage this resource for assistance in completing the stated activity, or utilize their activity and integrate the results into the overall plan?
- Resources available to implement plan: – Do you have the appropriate resources for the subject matter as needed within your department? (If not, is there subject matter expertise somewhere else in the organization?)
- If subject matter requires outsourcing, budget considerations and overall risk priorities may need to be re-evaluated

Developing an Internal Audit plan

Considerations

- Hours needed to complete the plan
- Projected timeframes
- Defined auditing or monitoring activities and determination as to whether they are outcomes or process oriented
- Flexibility incorporated into the plan to address changes in risk priorities and possibly unplanned compliance risks/crises which may need an immediate audit or monitoring to occur.

PART FIVE: RISK BASED AUDIT ENGAGEMENT

- Performing a risk based audit engagement
- Approaches for managing risks and evaluating controls
- Reporting risk based audit engagements

Performing a risk based audit engagement

- Reassess the risk assumptions of the auditable unit.
- Validate that the process in fact has sufficient risk to warrant assuring in this audit cycle.
  - Understand the business process and its objectives.
  - Identify the risks to the objectives. Usually, the client will do this in conjunction with their own process documentation.
  - Measure and prioritize risks.
  - Identify controls and evaluate the design.
  - Develop audit objectives and program.

Types and evaluation of controls

TYPES OF CONTROLS

- Directive: Controls that encourage desirable events to occur.
- Preventative: Controls that prevent undesirable events from occurring.
- Detective: Controls that detect undesirable events that have already occurred.
- Mitigating: Controls that compensate for a missing or costly control

EVALUATING CONTROLS

- Adequacy: Determine whether the process, as designed, provides reasonable assurance (operational auditing).
- Effectiveness: Determine whether the process is functioning as intended (transactional testing)

PART SIX: QUESTIONS & WRAP UP

Conclusion & Questions

Further enquiries you can reach me on:

hokorie@gmail.com

REFERENCES

IIA UK & Ireland (2015), *Governance of risk: Three lines of defence*. Retrieved from: https://www.iia.org.uk/resources/audit-committees/governance-of-risk-three-lines-of-defence/

The Institute of Internal Auditor (2016), *Assessing Cybersecurity Risk- Roles of the Three Lines of Defense*. Retrieved from: https://na.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/GTAG-Assessing-Cybersecurity-Risk-Roles-of-the-Three-Lines-of-Defense.aspx

Deloitte (2013), *Coso Internal Control Framework*, COSO Retrieved from: http://deloitte.wsj.com/riskandcompliance/files/2013/06/coso_table.png

Image, Retrieved from: http://www.wollongongfirstaid.com.au/workplace-audits-and-risk-management.htmlmanagement.html

Qfinance, *Best Practices in Risk-Based Internal Auditing*. Retrieved from: www.qfinance.com

IIA (2016) *Risk Based Audit-A value add perspective*, Florida