Institute of
Internal Auditors
Philippines

INTERNAL AUDIT, INTERNAL CONTROLS AND RISK MANAGEMENT

Myrna E. Amahan, CPA, CIA, CISA, CGEIT, MPM

- Let us spread the word about the value of internal auditing to organizations and the business community!!!

Session objectives

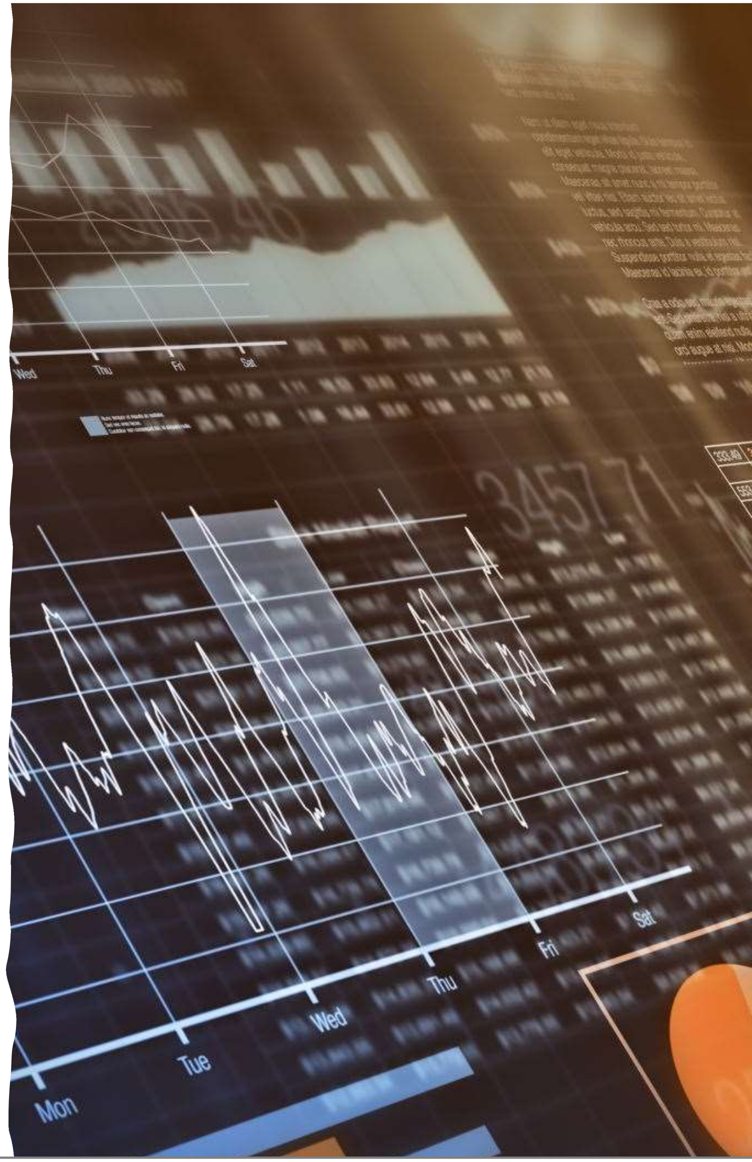
To discuss and share experiences on the following:

How to add more value to our respective organizations despite the challenges that IA faces.

Growing expectations from Internal Audit

- **P**ossess a laser sharp focus on risk horizon combined with **business knowledge, soft skills with increased reliance on technology** to add value from a foresight perspective.
- **Embrace** technology and go digital in order to provide reasonable assurance to Management and the Board. **Employ** tools and technology to reinforce audit objectives and desired outcomes, **remotely**.
- **Partner** with business functions to enable digitization.
- **Provide** a continuous assurance on the effectiveness of the risk design to the Audit Committee and the Board. Risk ownership and monitoring of the new norms of the business is still the prime responsibility of the Management and the Chief Risk Officer.
- **Shift** from **hindsight to insight and finally towards foresight**.

Remember the PEEPPS



Institute of Internal Auditors Philippines

Value of Internal Audit Assurance

Helps boards of directors and chief executives sleep at night.

Provides peace of mind that business risk is managed effectively

Do the processes and controls meet the needs of the business?

According to Norman Marks, this is the question he asks his internal auditors as they plan their audit engagements and this makes his internal auditors think and ask more questions such as:

- **What is management trying to achieve** with this business unit, activity, process, etc.?
- Does the way they are operating, which includes the **controls** they are relying on, provide reasonable assurance that they will be successful?
- That means that not only do they need to take the **right risks but seize the right opportunities**. Are they doing that?

Do the processes and controls meet the needs of the business?

- How well are they leading the organization and its people, obtaining **optimal performance** from both?
- Is there a **better way**? What can and should be improved?

According to Mr. Marks, answering these questions enabled his auditors to assess the **management of risks and opportunities and the related controls.**

The real challenge of internal audit

To ensure that **it is testing the controls that ensure the organization's major risks are effectively managed within organizational tolerances.**

Risk-based audit approach

The risk-based approach is suggested by the Institute of Internal Auditor's professional practice standards. Relevant IIA Standards state:

- **IIA Standard 2010** requires: "The chief audit executive must establish **risk-based plans** to determine the priorities of the internal audit."
- **IIA Standard 2010.A1 requires**: "The internal audit activity's plan of engagements must be based on a **documented risk assessment**, undertaken **at least annually**. The input of senior management and the board must be considered in this process."

A caveat to risk-based auditing approach (per Norman Marks)

It assesses the risks to the objectives of **auditable entities** (**the audit universe, a concept that should be retired**) instead of the risks to the objectives of the extended enterprise (**captured in a risk universe**).

The audit universe vs. risk universe

To address Mr. Marks' concern

During risk-based audit planning for the whole organization, the CAE assesses enterprise-wide risks to the enterprise-wide objectives.

During engagement level planning, the internal auditor-in-charge assesses the risks to the auditable entity/area to be audited. However, during this engagement risk assessment process, the considerations during risk assessment for the whole organization should also be considered. This is to ensure alignment.

IN DEFINING THE AUDIT OBJECTIVES

- Understanding the goals and objectives of an audit
  - Why is this audit being performed?
  - Why was it identified as a **risk**?
  - Why was it **deemed important enough to appear in the audit plan**?
- The above questions can be answered with the statements (which are really saying the same thing)
  - Because it **addresses a risk that could negatively impact the company's ability to achieve strategic goals/objectives**
  - The audit engagement is a part of an audit plan that is aligned with the company's strategic goals/objectives

Unwanted outcome of ineffective audit planning

Audit teams find themselves **performing too much work on controls for which they perceive there is little benefit.** It is therefore suggested that a **better definition is needed of what 'relevant to the audit' means.**

Audit teams only focusing on testing the consistent implementation of controls, **leaving out evaluating the appropriateness of the existing controls to address the risks the organization is facing**.

5 missteps to avoid when evaluating internal controls

(By Deana Thorps, CPA; Hiram Hasty, CPA, CGMA; and Bob Dohrer, CPA, CGMA
July 1, 2019 Journal of Accountancy)

1. Assuming the client has no controls
2. Not understanding which controls are relevant to the audit
3. Stopping after determining whether controls exist
4. Improperly assessing control risk
5. Failing to link further procedures to control-related risks

Tips to avoid these missteps

When performing future audit engagements, auditors should be sure to:

- Obtain a **robust understanding** of the client's system of internal control;
- Determine if there are **process gaps**;
- Identify controls relevant to the audit;
- Evaluate the **design effectiveness** of each relevant control and determine whether the controls have been implemented as designed;
- Identify and assess the client's risks of **material misstatement** (including **control risk**) at the assertion level;
- Design and perform audit procedures that are **responsive** to the assessed risks; and
- Document the **linkage** between the assessed risk and the audit procedures.

Risk Ownership

Risk Owner: **The individual who is ultimately accountable for ensuring the risk is managed appropriately**. There may be multiple personnel who have direct responsibility for, or oversight of, activities to manage each identified risk, and who collaborate with the accountable risk owner in his/her risk management efforts.

The risk owner has the **necessary level of authority** to be able to spend resources and to be able to make sure he or she can task people to undertake the treatment strategies that might be directed towards that particular risk.

Avoid risk will fall through the cracks

A designated risk owner ***ensures someone in the organization is accountable for the risk***.

If there is not one person or a group charged with managing a risk, then by default, the entire organization will own the risk, and therefore it is highly likely the risk will fall through the cracks (a/k/a nothing will be done).

Having a risk owner is an important step toward ensuring that a response plan is developed and acted upon in a timely manner.

Control Owner

Responsible for the:

- oversight of the control to make sure it is effective.
- measurement or directing the measurement of the effectiveness of that control
- updating and reviewing that particular control over time
- informing not only the risk owner but also the executive for very important controls where that control is starting to become less effective

Every single control within an organization needs to have a control owner.

Treatment Owner

Responsible for undertaking the treatment plan or the treatment strategy that they have been directed to do.

The treatment owner is not necessarily going to be the risk owner or the control owner, in most cases.

Constant Communication needed among the 3- Risk, control and treatment owners

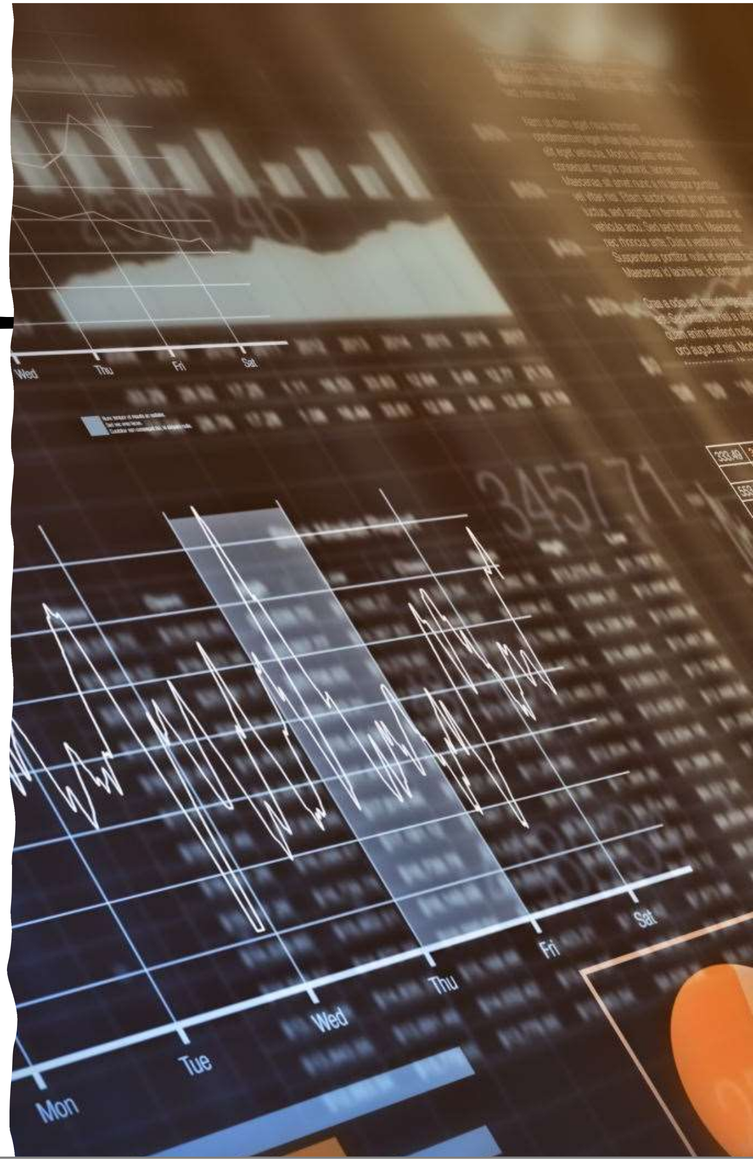
- Each of them needs to know what the others are doing. There needs to be constant communication – between and among the three owners.
- That is particularly the case for risks within the organization where the consequences of failure are of the highest level.
- Organizations need to assign ownership to risks.
- Control ownership also needs to be allocated to a single individual and treatment strategies, like the other two, single individuals.
- This should be indicated in the company's risk register. Otherwise, nothing is going to happen.

Remember, risks without owners will never be managed. Also, controls and treatments without owners will never be done.

Growing expectations from Internal Audit

- **Possess** a laser sharp focus on risk horizon combined with **business knowledge, soft skills with increased reliance on technology** to add value from a foresight perspective.
- **Embrace** technology and go digital in order to provide reasonable assurance to Management and the Board. **Employ** tools and technology to reinforce audit objectives and desired outcomes, **remotely**.
- **Partner** with business functions to enable digitization.
- **Provide** a continuous assurance on the effectiveness of the risk design to the Audit Committee and the Board. Risk ownership and monitoring of the new norms of the business is still the prime responsibility of the Management and the Chief Risk Officer.
- **Shift** from **hindsight to insight and finally towards foresight**.

Remember the PEEPPS



Institute of Internal Auditors Philippines

Sample Internal Audit Function's Mission

To provide independent and objective opinions and insights (assurance and consulting engagements) on what matters now and in the near future through an agile way.


IF AT FIRST YOU DON'T
SUCCEED
TRY DOING WHAT YOUR
AUDITOR
SAID IN THE FIRST PLACE

UnionBank

THANK YOU!