UK INTERNAL AUDIT'S (UKIA) PROTOCOL FOR AUDITEE ACCEPTANCE OF RISKS

Martin Anibaba, Audit Director

University of Kentucky

AN EQUAL OPPORTUNITY UNIVERSITY

RISK EVALUATION PROCESS

RISK – UKIA DEFINITION

Risk is…

The uncertainties that the organization must understand and effectively manage to execute its strategies, achieve its objectives and performance goals and create value.

- Marsh Risk Consulting

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.

- *The Institute of Internal Auditors*

The exposure of someone or something valued to danger, harm or loss.

- *Oxford Dictionary*

Any obstacle in the way of achieving the university's objectives.

- UKIA

University of Kentucky

ENTERPRISE RISK MANAGEMENT (ERM) - OVERVIEW

A structured, consistent and continuous process that is applied across the entire organization and brings value by:

- Proactively identifying, assessing and prioritizing material risks
- Developing and deploying effective mitigation strategies
- Aligning with strategic objectives and business processes
- Embedding key components into the organization's culture:
  - Risk ownership, governance and oversight
  - Reporting and communications
  - Leveraging technology and tools

Enterprise Risk Workshop Summary Report
Marsh Risk Consulting

"UKIA effectively participates in risk management activities within UK from an assurance and advisory perspective."

– 2020 Quality Assessment Review Report by the Institute of Internal Auditors

University of Kentucky

INTERNAL AUDIT RISK-RELATED STANDARDS

From the Institute of Internal Auditors International Professional Practices Framework

Standard 2120 – Risk Management

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

Standard 2010 – Planning

The chief audit executive must establish a risk-based plan to determine the priorities of the internal audit activity, consistent with the organization's goals.

Standard 2210.A1 – Engagement Objectives

Internal auditors must conduct a preliminary assessment of the risks relevant to the activity under review. Engagement objectives must reflect the results of this assessment.

Standard 2600 – Communicating the Acceptance of Risks

When the chief audit executive concludes that management has accepted a level of risk that may be unacceptable to the organization, the chief audit executive must discuss the matter with senior management. If the chief audit executive determines that the matter has not been resolved, the chief audit executive must communicate the matter to the board.

RISK CATEGORIES – INTERRELATEDNESS

UK's Risk Categories

Enterprise Risk Workshop Summary Report
Marsh Risk Consulting

1. Financial
2. Operational
3. Legal/Regulatory
4. Technology
5. Strategic
6. Human Capital

UKIA Business Risk Factors

1. Public Exposure
2. External Factors
3. Materiality
4. Audit Interval
5. Control Environment I
6. Control Environment II
7. Management Requests

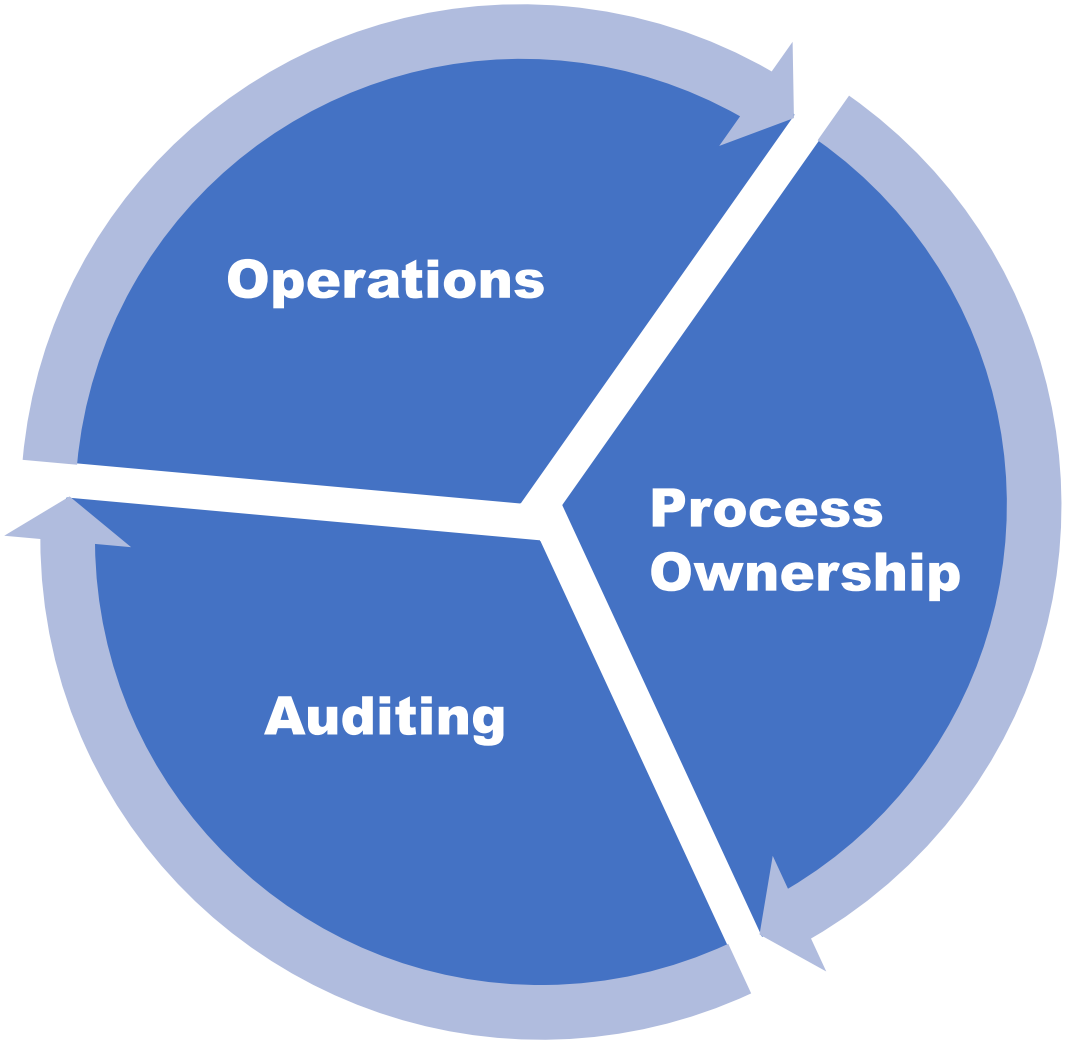
STAKEHOLDERS' RESPONSIBILITIES

1st Line of Defense: Unit

- Executes the processes

2nd Line of Defense: Process Owner

- Develops the policies to ensure regulatory adherence
- Monitors units' activity related to the process under their purview



3rd Line of Defense: UK Internal Audit

- Reviews processes and practices to assess risk
- Communicates the risk
- Obtains commitment on remediation from the Auditee
- Evaluates the effectiveness of the Auditee's remediation strategy
- Unmanaged risk reported to ACC

UKIA'S RISK PROTOCOL

UKIA's methods include:

- Collaboration with process owners (e.g., University Financial Services, UK Information Technology Services, University Budget Office)

- Check-ins with the audit client
  - Typically, 90 days
  - Conducted by the chief audit executive and communications manager

- Conduct follow-up audits/reviews
  - Typically, 12-18 months

INDUSTRY RISK MANAGEMENT

SARA Model

Sharing (Transference)
Assign or move the risk to a third party

Avoidance
Completely eliminate risk

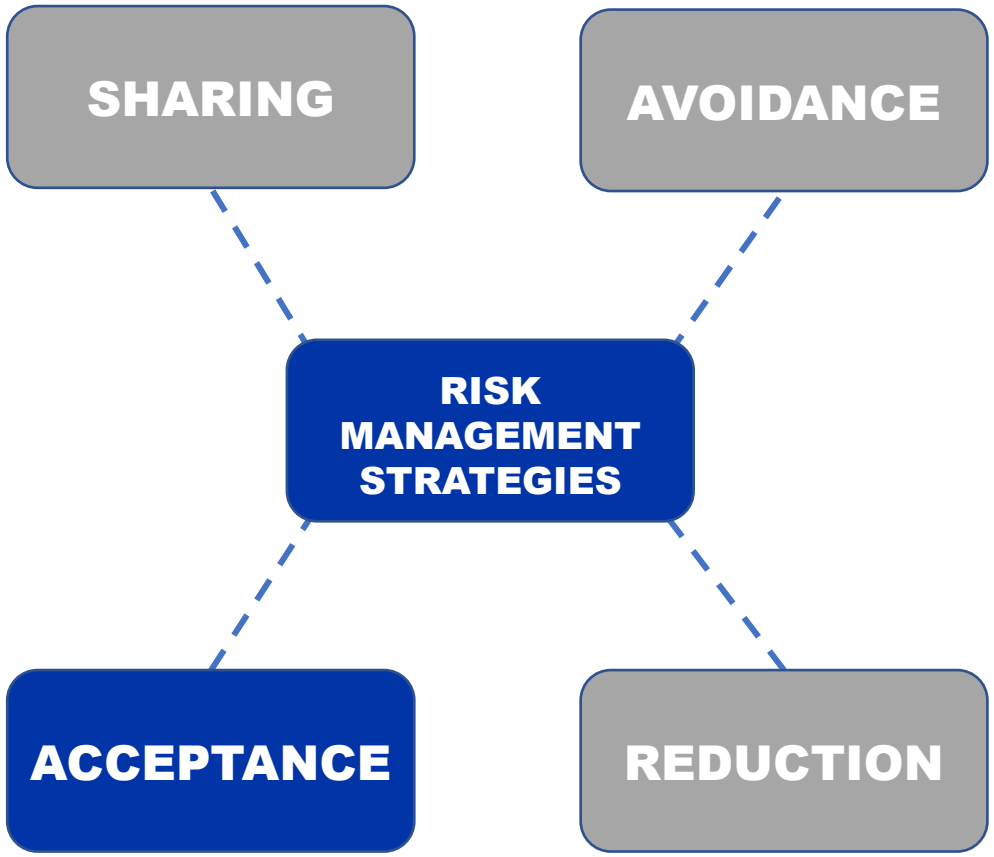
Acceptance
Acknowledge the risk and choose not to transfer, reduce or avoid

Reduction
Reduce the likelihood or impact of risk

INDUSTRY RISK MANAGEMENT

SARA Model

Sharing (Transference)
Assign or move the risk to a third party



Avoidance
Completely eliminate risk

Acceptance
Acknowledge the risk and choose not to transfer, reduce or avoid

Reduction
Reduce the likelihood or impact of risk

UKIA'S PROTOCOL FOR AUDITEE "ACCEPTANCE OF RISKS"

Default position:

"Acceptance of Risk" = Non-Remediation / Non-Mitigation

Professional Standards Requirement

Standard 2600 – Communicating the Acceptance of Risks

When the chief audit executive concludes that management has accepted a level of risk that may be unacceptable to the organization, the chief audit executive must discuss the matter with senior management. If the chief audit executive determines that the matter has not been resolved, the chief audit executive must communicate the matter to the board.

UKIA's protocol for communicating the acceptance of risks:

When an auditee decides on non-remediation (acceptance) of the identified risk, UKIA will escalate to the appropriate stakeholders to include but not limited to the senior management and the Audit and Compliance Committee of the Board of Trustees.

UKIA experience

- In the few cases this has occurred over the years, the initial "acceptance of risk" has always been reversed prior to audit report issuance.
- This is a rare occurrence.

RISK REMEDIATION – COMPUTATION AND REPORTING

UKIA Metric #6

- This metric measures how many of UKIA's findings have been remediated.
- This gives UKIA insight into the level of risk mitigation throughout the university.
- UKIA reports as one of the seven metrics to the Audit and Compliance Committee.

Formula

This metric is calculated by ranking the mitigation on the following scale:

3 = Satisfactory (S)
2 = Partially Satisfactory (PS)
0 = Unsatisfactory (U)

The ranking number is then multiplied by the number of findings with that score, and the results are then added together. The remediation score is that sum divided by the highest possible sum (found by using 3 as the rating number for all the findings).

$$\frac{3\ (\#\ \text{of S findings}) + 2\ (\#\ \text{of PS findings}) + 0\ (\#\ \text{of U findings})}{3\ (\text{total}\ \#\ \text{of findings})}$$

QUESTIONS

University of Kentucky

AN EQUAL OPPORTUNITY UNIVERSITY

UK INTERNAL AUDIT MISSION STATEMENT

To support UK in its pursuit of excellence by providing expert analyses and advice to champion the achievement of management objectives.