Risk Based Internal Auditing & Enterprise Risk Management

PRESENTERS:

JUDITH NELSON, UNIVERSITY MANAGEMENT AUDITOR

DWIGHT WALTERS, MANAGER, PROJECTS & COMMERCIAL OPERATIONS
Risk Based Internal Auditing & Enterprise Risk Management

What we will cover today:

1. Risk-based Internal Auditing – the new approach for Management Audit

2. Enterprise Risk Management (ERM)
   a) An Understanding of ERM
   b) The ERM sub-component of the UWI Institutional Strengthening Project
RISK-BASED INTERNAL AUDITING (RBIA)

THE NEW APPROACH FOR MANAGEMENT AUDIT

Judith Nelson
Why are we adopting a Risk Based approach to Internal Auditing?

The key objective of Management Audit’s Strategic Action Plan 2010 to 2013 is to successfully pass an external Quality Assurance Review (QAR) within 48 months and be able to use in all our audit reports:

““Conforms with the International Standards for the Professional Practice of Internal Auditing””
The UMAD strategic objective requires that we:

1. Change our ways of working to align with the IIA International Standards of Professional Practice, Code of Ethics & the Definition of Internal Audit.

2. Be subject to review by an external party (yes, audit will be audited) who assesses our compliance.
2010 – Planning: The chief audit executive should establish risk-based plans to determine the priorities of the internal audit activity, consistent with the organization’s goals.
RBIA is the methodology which provides **assurance** that risks are being managed to within the organisation’s risk appetite.
5 Key Internal Audit Roles

1. Giving assurance that the processes used by management to identify all significant risks are effective.

2. Giving assurance that risks are correctly assessed (scored) by management, in order to prioritise them.

3. Evaluating risk management processes, to ensure the response to any risk is appropriate and conforms to the organisation’s policies.

4. Evaluating the reporting of key risks, by managers to directors.

5. Reviewing the management of key risks by managers to ensure controls have been put into operation and are being monitored.
Risk Based Internal Auditing & Enterprise Risk Management

WHAT IS RISK?
Risk Based Internal Auditing & Enterprise Risk Management

- Risk is defined by the IIA’s International Standards of Professional Practice as:

  “The uncertainty of an event occurring that could have an impact on the achievement of objectives.”

- Risk is defined by ISO 31000 as:

  “the effect of uncertainty on objectives”
Risk Based Internal Auditing (RBIA)

RBIA starts with the **business objectives** and then focuses on those **risks that have been identified by management** that may hinder their achievement.

How does this work?
The University has entity-wide strategic objectives – STRIDE.

Not all campuses, faculties and administrative units have developed their own strategic objectives, however we have general alignment across the University to STRIDE.

Where the entity has not developed their own strategic objectives (*which must align to STRIDE*), Management Audit defaults to STRIDE.
The process of *risk identification* and assessment is less robust at the UWI but you will hear more about it as we get into ERM.
If risks have not been identified and assessed by management what do we do?

Management Audit does its own risk assessment.
Here is the list of Higher Education risks that Management Audit uses to do risk assessment:

- Financial Risk
- Information System Risk
- Student Experience Risk
- Human Resources Risk
- Reputational Risk
- Commercial Risk
- Audit History Risk
- Estate and Facility Risk
- Strategic Risk
- Governance Risk
Risk assessment & prioritisation is done at 2 levels:

- At the organisational level to develop the annual audit plan (e.g. at Campus level)

- At the engagement level for each audit engagement we do. (e.g. at auditable entity level)
Within the context of RBIA, internal audit can only provide **assurance** where a risk management framework is in place: all other work is consultancy.
Therefore to accomplish our strategic objectives of full compliance with the IIA standards, we must work with the UWI management in the establishment of a robust Risk Management Framework.

Enterprise Risk Management (ERM)
Risk Based Internal Auditing & Enterprise Risk Management

AN UNDERSTANDING OF ERM

Dwight Walters
What You don’t know about corporate ‘Enterprise Risk Management’ may hurt you!!

- Remember Enron; Barings Bank: These organizations were crippled or destroyed by failure of control mechanisms.

- All these and growing number of events are debacles that might have been avoided if effective ERM programs had been in place.
Risk Based Internal Auditing & Enterprise Risk Management

What are some of the major risks faced by the University?

- Data Privacy
- Financial Misconduct
- Student Misconduct
- Financial Aid

- Technology Reliability
- Research & Grant Misconduct

- Legal & Regulatory
- Strategic Information
- Environment, Health & Safety
- Employee Skills & Retention

- Access to Funds
- Timely/Accurate Financial Information
So what exactly is ERM?

- Start by admitting that ERM is difficult to define exactly (a relatively new management discipline that is constantly changing).
- We know that Risk Management is not a new concept!!
- Organizations have been able to manage isolated ‘pockets or silos of risk’ for many years.
- In sophisticated developed capital markets ‘derivative instruments’ have helped manage the ups and downs of movements is currencies, interest rates, commodities prices and equities.
- Organizations have also been able to transfer risks though insurance – using a wide array of products (including Captive Insurance) as we have see in a previous presentation.
So what exactly is ERM?

Examples of differences between the ‘silo’ approach and the ERM approach.

- One campus may be long in certain foreign currency and another campus may be short in that same currency. Using separate currency hedges while seemingly advisable from the point of view of the individual campus management, may be unreasonable for the University enterprise as a whole. As these risks represent a “natural hedge” against each other.
So what exactly is ERM?

Another Examples of differences between the ‘silos’ approach and the ERM approach.

A classic case of an insurer selling both life insurance and annuity business to similarly situated customers and thereby naturally hedging away its mortality risks. To separately hedge mortality risk on these products (e.g. through reinsurance) would be cost inefficient.
**Enterprise Risk Management** is meant to have a broad meaning as an all-encompassing term to describe an integrated and enterprise-wide comprehensive processes that include: 1.) **emergency response**; 2.) resumption; 3.) recovery; and 4.) restoration

<table>
<thead>
<tr>
<th>Contingency Planning</th>
<th>Business Impact Analysis</th>
<th>Business Recovery</th>
<th>Business Resumption Planning</th>
<th>Command Centers</th>
<th>ERM Perspective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crisis Communication</td>
<td>Crisis Management</td>
<td>Disaster Recovery</td>
<td>Emergency Management &amp; Response</td>
<td>Strategic Risk</td>
<td></td>
</tr>
<tr>
<td>Information Security</td>
<td>Mitigation Planning</td>
<td>Risk Control</td>
<td>Risk Financing &amp; Insurance</td>
<td>Operational Risk</td>
<td></td>
</tr>
<tr>
<td>Risk Management</td>
<td>EHS</td>
<td>Police</td>
<td>Safety &amp; Security Council</td>
<td>Reputation Risk</td>
<td></td>
</tr>
<tr>
<td>Computer Security</td>
<td>Business Continuity</td>
<td>Regulatory Compliance</td>
<td>Safety &amp; Security Council</td>
<td>Regulatory or Contractual Risk</td>
<td></td>
</tr>
<tr>
<td>Student Housing</td>
<td>Academic Administration</td>
<td>Operations</td>
<td>Risk Mgmt Adhoc Committee</td>
<td>Financial Risk</td>
<td></td>
</tr>
</tbody>
</table>

---

**Risk Based Internal Auditing & Enterprise Risk Management**

---

**Contingency Planning**
- Crisis Communication
- Crisis Management
- Disaster Recovery
- Emergency Management & Response

**Exercising & Training**
- Information Security
- Mitigation Planning
- Risk Control
- Risk Financing & Insurance

**Safety & Security**
- Risk Management
- EHS
- Police

**Event Management**
- Computer Security
- Business Continuity
- Regulatory Compliance
- Safety & Security Council

**Fire Protection**
- Student Housing
- Academic Administration
- Operations
- Risk Mgmt Adhoc Committee

---

**ERM Perspective**
- Strategic Risk
- Operational Risk
- Reputation Risk
- Regulatory or Contractual Risk
- Financial Risk
So what exactly is ERM?

- Where ERM also comes in is where organizations manage the risks that **defy easy measurement** or a framework for management.

- These include crucial risks related to **reputation**; **day-to-day operational procedures**; **supply chain**; **legal and human resources management** (all fall under the ERM umbrella).
So what exactly is ERM?

**Upside vs. Downside Risks**

- Traditional approach has been to focus on the **downside** – In the past tended to take a defensive posture towards risks. Where risk viewed as situations to avoided. (e.g. the losses from currency or interest rate trades in financial markets, or financial losses that might be caused by disruption in a supply chain) – remains a *legitimate strategy*.

- ERM says we should also consider the ‘**upside**’ of risks: considering competitive opportunities and strategic advantages that might arise out of astute management of risk and making collectively ‘better decisions’.
Risk Based Internal Auditing & Enterprise Risk Management

Keep Us Out of Trouble
- Reputation Damage
- Regulatory expansion

Make Our Business Better
- Fines and Settlements
- Criminal Indictments
- Better stakeholder relations
- Risks are identified and monitored
- Improved reputation
- Controls are optimized

Goal
So what exactly is ERM?

Risk as Opportunity: Some potentially competitive upside opportunities for the University

- Centralized Treasury Management
- Exploiting currency triangular arbitrage opportunities cross-campus
- Investment Pooling?
- Captive Insurance
- Use of derivative instruments in informed risk taking
We cannot Manage what we have not Measured!!

How do we measure Risk?
So what exactly is ERM?

Risk Measurement Issues:

- Lets keep it **SIMPLE!!** Aim for ‘*directional correctness*’ in evaluating risk.

- Having **identified** a risk, how an organization **responds** to the enterprise-wide risks should depend on the **impact** of that risk event and the **likelihood** (probability) of the event occurring.

- Risk Measure (product) = Impact x likelihood

- The **higher** the ‘product’ the **high the risk**
So what exactly is ERM?

Risk Measurement Issues:
Example of a scale (5 x 5 matrix) used for impact and likelihood

**Impact:**
1. Insignificant
2. Minor
3. Moderate
4. Serious
5. Very serious

**Likelihood:**
1. Very Low
2. Low
3. Medium
4. High
5. Very High

The combined scores on the 5 x 5 matrix will give indicative scores ranging from 1 to 25 depending on the severity of the risk.
So what exactly is ERM?

How to respond to the Risk Measurement:
- The response is gauged by the significance of the risk measure

<table>
<thead>
<tr>
<th>Risk measure</th>
<th>Response Guide</th>
</tr>
</thead>
<tbody>
<tr>
<td>0- 6 Low</td>
<td>Low level of risk; should much attention, but should be reviewed at least annually</td>
</tr>
<tr>
<td>8- 12 Medium</td>
<td>Medium level of risk, monitored and reviewed annually as a minimum, monthly if necessary</td>
</tr>
<tr>
<td>14 – 20 High</td>
<td>High level of risk, should be constantly monitored and reviewed quarterly</td>
</tr>
<tr>
<td>Over 20 – very serious</td>
<td>Top level risk, constantly monitored and reviewed monthly</td>
</tr>
</tbody>
</table>
So what exactly is ERM?

- **High Impact**/High Likelihood
- Green: Low Impact/Likelihood
- Yellow: Moderate Impact/Likelihood
- Red: High Impact/Likelihood

Risk Based Internal Auditing & Enterprise Risk Management
Risk Based Internal Auditing & Enterprise Risk Management

- Collapse of student numbers
- Gov’t Contb fall-off
- Financial Systems fail
- Research team falsify results
- Major IT project overspent
- University Sued for dismissal
So what exactly is ERM?
How should we respond to risk assessment

- Before we respond we must determine how much risk we are willing to tolerate (risk appetite).
- Risk thresholds should provide the trigger for action.
- Thresholds for both each risk event and a global threshold.
There are a range of responses available to the University from its assessment of its overall level of risk or ‘exposure’:

- **Reduce risk** – take action to reduce either the likelihood or impact
- **Accept risk** – when the probability and impact are low
- **Transfer risk** – to third party e.g. insurance.
- **Terminate risk** – identifying action to eliminate the risk

The response should be proportional to the risk.
So what exactly is ERM?

**Lets Recap:** Putting it all together

- **ERM** – ‘E’ is about the enterprise (organization-wide) not only ‘silos’ within.
- **ERM** – ‘R’ is about risk(threats) that could affect the organization either adversely or beneficially.
- **ERM** – ‘M’ is about the management of these risks which need to be measured (quantified) before; not only individually but also **globally** for the enterprise.
So what exactly is ERM?

Finally a Definition:

ERM is the process of identifying and analyzing risk from an integrated, companywide perspective. It’s designed to identify potential events or actions (i.e. risks!) that may adversely or beneficially affect an organization, and to manage these risks to provide reasonable assurance that the organization’s objectives will be achieved.
Risk Based Internal Auditing & Enterprise Risk Management

THE ERM SUB-COMPONENT OF THE UWI INSTITUTIONAL STRENGTHENING PROJECT

Judith Nelson
THE DEVELOPMENT AND IMPLEMENTATION OF AN ENTERPRISE RISK MANAGEMENT PROGRAMME AT THE UNIVERSITY OF THE WEST INDIES

(ITEM (III) OF THE INSTITUTIONAL STRENGTHENING SEGMENT OF THE UNIVERSITY OF THE WEST INDIES ENHANCEMENT PROJECT)
The scope of the engagement is:

To design a risk management framework appropriate to the Universities’ structure and governance framework.

To develop and document a manual documenting all approved policies, procedures, forms, registers and other documents required for the ERM framework.

To design and document an agreed compliance framework to monitor the risk management process.
Risk Based Internal Auditing & Enterprise Risk Management

To guide and facilitate the orderly and effective implementation of the agreed framework

Staff to be fully trained and educated on the relevant ERM operational processes, their duties & responsibilities; core skill sets, forms and registers for all levels of staff in all operations and locations of the University.

All required technical and functional training for users of the ERM Information system.
Risk Based Internal Auditing & Enterprise Risk Management

To conduct an evaluation and advise on the selection of the proposed ERM information system

To guide and facilitate the orderly and effective implementation of the selected ERM information system and undertake technical & functional user training
Risk Based Internal Auditing & Enterprise Risk Management

Where we are at today!
The End
Q&A